BeWAN Secure série 50

Guide de l'utilisateur

Avertissement

Les informations contenues dans ce manuel sont susceptibles de modification sans préavis.

LE CONSTRUCTEUR NE PEUT ETRE TENU POUR RESPONSABLE SI UNE NON-CONFORMITE PARTIELLE APPARAIT ENTRE CE MANUEL ET LE PRODUIT QU'IL DECRIT, NI DES DOMMAGES ACCIDENTELS CONSECUTIFS A L'UTILISATION DE CEUX-CI.

Le manuel et le Logiciel fournis sont protégés par les lois de Copyright et ne peuvent être copiés ou distribués de quelque façon et pour quelque usage que ce soit. Ce manuel est régi par les modalités et les conditions affichées dans le programme d'installation que vous devez avoir acceptées avant de l'utiliser. L'utilisation du Logiciel et de sa Documentation est mono-produit et pour un usage personnel uniquement. Toute utilisation à des fins commerciales est strictement interdite. La violation de ces règles peut entraîner des poursuites judiciaires et la personne concernée sera tenue responsable sur le plan économique de tout préjudice et perte subie par le titulaire du copyright.

Copyright © 2005-2006, BeWAN systems. Tous droits réservés.
Edition juillet 2006.

Marques déposées et copyright :

- BeWAN et le logo BeWAN systems sont des marques déposées de BeWAN systems.
- Microsoft et Windows sont des marques déposées de Microsoft Corporation aux Etats-Unis et/ou dans d'autres pays.

De même, les noms des produits cités dans ce manuel à des fins d'identification peuvent être des marques commerciales, déposées ou non par leurs sociétés respectives.

Le matériel que vous avez acheté ne doit pas être jeté avec les ordures ménagères. Vous devez le rapporter à votre distributeur, en cas de remplacement, ou le déposer dans un point de collecte approprié pour le traitement, la valorisation ou le recyclage des déchets EEE (Equipements Electriques et Electroniques).

Vous faîtes ainsi un geste pour l'environnement, en contribuant à la préservation des ressources naturelles et à la protection de la santé humaine.

Table des matières

1. Avant-propos 5

Introduction 5

Fonctionnalités 6

Contenu de l'emballage 6

Configuration requise 7

Assistance technique 7

Précautions d'utilisation 7

Emplacement 7

Entretien et maintenance 8

Alimentation et câbles 8

2. Boîtier et voyants lumineux 9

Face avant 9

Face arrière 10

3. Installation et configuration rapide 11

Raccordement des BeWAN Secure série 50 11

Connexion aux BeWAN Secure série 50 12

Configuration rapide 13

Interface WAN 13

Interface LAN 22

Mot de passe de l'administration Web 22

Protocole de temps (NTP) 22

4. Administration Web 23

Configuration rapide 25

Interfaces 25

Interface LAN 25

Interface WAN 26

Interface Wireless (modèles BeWAN Secure 50G et M50G) 27

Filtrage de contenu 33

Filtrage de mots clés 33

Blocage d'URL 34

IP autorisées 34

Ports filtrés 35

Réglages avancés 36

DHCP 36

DNS dynamique *38*
Mappage des ports *39*
Pare-feu *40*
Serveur virtuel *44*
Gestion de la bande passante *47*
VPN *52*
SIP *81*
Routes statiques *82*
Table de traduction d'adresses MAC (Table ARP) *84*
Table des noms d'hôte *86*
Wake On LAN *87*
VLAN *88*
Surveillance des emails 89
Groupes de mail *89*
Serveurs de mails *90*
Fonction Webcam 91
Configuration de la webcam *91*
Webcam en direct *94*
Serveur FTP 95
Paramètres FTP *95*
Compte FTP *96*
Connexion au serveur FTP depuis Windows *99*
État du serveur FTP *107*
Maintenance 108
Administration système *108*
Information système *110*
Langue *110*
Heure *111*
Périphériques USB *112*
Utilisateurs en ligne *113*
Firmware & Configuration *114*
Ping *116*
Traceroute *117*
Log *118*
Redémarrer 119
Sauvegarder 119
Déconnecter 119
5. Serveur d'impression (sous Windows 2000 et XP) 120
Annexes 127
Liste des webcams compatibles 127
Liste des imprimantes compatibles 132

1. Avant-propos

Introduction

Les BeWAN Secure série 50 sont des routeurs professionnels conçus pour connecter un réseau d'entreprise à Internet via un modem externe haut débit. Ils sont parfaitement adaptés aux différents besoins des PME et administrations publiques en matière de sécurité, de partage des ressources et de mobilité :

- partage d'un accès Internet haut débit via 1 port WAN 10/100 pour le raccordement d'un modem externe xDSL, câble, WiMax, satellite ;
- création ou extension d'un réseau local câblé, grâce au commutateur 4 ports 10/100, ou sans fil lorsque le modèle intègre en plus un point d'accès Wi-Fi ;
- pare-feu complet et paramétrable disposant notamment des fonctions SPI (***S**tatefull **P**acket **I**nspection*), DoS/DDoS (Déni de Service) et d'un système de filtrage performant ;
- création de réseaux privés virtuels sécurisés jusqu'à 50 tunnels VPN IPSec ou 10 tunnels VPN PPTP en mode client afin d'interconnecter des réseaux distants via Internet, entre une société et ses filiales par exemple ;
- Multi-services. Serveur FTP de stockage, serveur d'imprimante et de vidéo-surveillance via 4 ports USB 2.0 (modèles M50 et M50G uniquement) pour le raccordement de périphériques de stockage ou d'acquisition (disque dur, clé, baladeur MP3, appareil photo…), imprimantes et webcams ;
- Qualité de Service (QoS). Garantie d'une bande passante aux différents utilisateurs et gestion des priorités entre les applications.

La série BeWAN Secure 50 se compose de 4 modèles :

- ✓ BeWAN Secure 50 Routeur VPN
- ✓ BeWAN Secure 50G Routeur VPN Wi-Fi
- ✓ BeWAN Secure M50 Routeur VPN multi-services (4 ports USB)
- ✓ BeWAN Secure M50G Routeur VPN multi-services et Wi-Fi

Fonctionnalités

- Processeur MIPS 167 MHz
- Pare-feu
    - ✓ Pare-feu SPI (**S**tateful **P**acket **I**nspection)
    - ✓ Protection DoS (***D**enial **o**f **S**ervice*)
    - ✓ Véritable filtrage des données
- HyperQoS (*Hyper-Quality of Service*) et HyperSHAPER
- VPN (**V**irtual **P**rivate **N**etwork) IPSec
    - ✓ Prend en charge les méthodes de cryptage 3DES 168 bits et AES 128/192/256 bits
    - ✓ Prend en charge le hachage MD-5 et SHA-1
    - ✓ Prend en charge la gestion des clés IKE
    - ✓ Prend en charge 10 tunnels VPN PPTP et 50 tunnels VPN IPSec
    - ✓ Compatible avec les autres produits VPN IPSec
- Prise en charge de 4 ports USB 2.0, logiciel d'application USB intégré (modèles BeWAN Secure M50 et M50G)
- Serveur d'impression, de webcam et FTP intégrés (modèles BeWAN Secure M50 et M50G)
- Prise en charge d'une interface Web en français et en anglais avec possibilité de basculement à tout moment
- Quatre ports Ethernet intégrés
- Prise en charge de l'interface Ethernet Auto MDI/MDI-X
- Prise en charge des normes sans fil 802.11b/g (modèles BeWAN Secure 50G et M50G)

Contenu de l'emballage

- Un routeur de la série BeWAN Secure 50
- Un adaptateur secteur
- Un câble Ethernet (1 mètre)
- Un CD contenant la documentation au format PDF
- Une antenne externe destinée à être vissée à l'arrière du routeur (modèles BeWAN Secure 50G et M50G)
- Une carte contenant les Conditions Générales de Garantie

Configuration requise

- Une connexion Internet RJ45
- Un PC équipé d'une carte réseau 10/100 Mbps avec prise en charge du protocole TCP/IP
- Un navigateur tel que Mozilla 1.0, Netscape 7.0 ou Internet Explorer 6.0 et ultérieurs
- Tension de 100 - 240 V

Avertissement : afin d'éviter les effets potentiellement néfastes du rayonnement, il est recommandé de tenir le routeur éloigné à plus de 20 cm.

Assistance technique

La série BeWAN Secure 50 et sa documentation ont été conçues dans un souci de simplicité, afin de pouvoir être utilisés tant par les particuliers que par les professionnels.

Avant de procéder à l'installation du routeur , nous vous conseillons d'enregistrer votre produit sur le site Web de BeWAN systems (http://www.bewan.fr) pour bénéficier de l'ensemble des services BeWAN systems.

Si vous rencontrez des difficultés, contactez votre revendeur afin qu'il vérifie votre configuration. Sinon, une assistance technique sur le matériel est assurée par le Support Technique de BeWAN systems au **08 92 16 22 92*** (Coût de la communication : Tarif Audiotel 0,34 € TTC/min).

Remarque : pour toute information sur le service d'assistance technique de BeWAN systems ou pour bénéficier des mises à jour du produit, consultez le site Web de BeWAN systems.

Précautions d'utilisation

Lisez attentivement les instructions de sécurité suivantes avant d'installer ou d'utiliser le routeur. Veillez à respecter rigoureusement les précautions d'emploi.

Emplacement

- Évitez d'utiliser, de placer et de conserver le routeur dans des endroits exposés à une lumière intense ou à des températures élevées ou près de sources de chaleur.
  Des températures élevées risquent de déformer le boîtier. La température maximum ne doit pas dépasser 40°C.
- Evitez d'installer le routeur dans un endroit humide et poussiéreux. Conservez le routeur dans un endroit sûr et bien ventilé.
- Ne placez pas le routeur sur un élément non stable. Si le routeur tombe, cela pourrait causer de sérieux dommages.

* depuis la France uniquement. Voir les horaires d'ouverture sur www.bewan.fr

- L'emplacement de la prise de courant secteur doit être facilement accessible. La tension secteur doit correspondre aux indications figurant sur la plaque signalétique de l'adaptateur électrique.
- Conservez le routeur hors de portée des enfants.

Entretien et maintenance

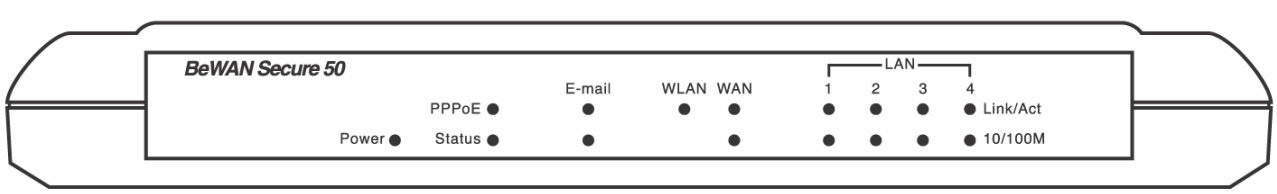
- Veillez à ne pas ouvrir, désassembler ou modifier une partie du routeur.
  Tout désassemblage ou modification pourrait provoquer une forte décharge électrique. Les inspections internes, les modifications et les réparations doivent impérativement être effectuées par des techniciens agréés et qualifiés. L'ouverture du routeur ou toute modification interne entraînera la perte de la garantie.
- Avant de nettoyer le boîtier, le produit ne doit pas être alimenté.
- Pour nettoyer le boîtier, n'utilisez pas certains produits chimiques pouvant endommager les matières plastiques.
  N'utilisez pas de substances contenant de l'alcool, du benzène, du diluant ni d'autres produits inflammables.
- Ne mettez pas le boîtier en contact avec de l'eau ou d'autres liquides.
  Aucun liquide ne doit pénétrer à l'intérieur du routeur. Si la partie externe de l'appareil entre en contact avec un liquide, essuyez-le à l'aide d'un chiffon doux et absorbant. Si un liquide ou une substance quelconque pénètre à l'intérieur du routeur, éteignez-le immédiatement ou débranchez le cordon d'alimentation de la prise électrique pour éviter un court-circuit.

Alimentation et câbles

- N'utilisez que les accessoires d'alimentation recommandés. L'utilisation de sources d'alimentation autres que celles recommandées pour ce matériel pourrait entraîner une surchauffe ou une déformation de l'appareil, et provoquer entre autres un incendie ou une décharge électrique.
- Veillez à ce que les câbles soient dans une position qui évite que quelqu'un puisse trébucher ou marcher dessus. Ne tentez pas d'acheminer les câbles dans un passage ou un endroit susceptible de les pincer.
- Ne touchez pas le cordon d'alimentation si vos mains sont mouillées Vous risqueriez de recevoir une décharge électrique.
- Lorsque vous débranchez le cordon, tenez la partie solide de la prise.
  En tirant sur la partie flexible du cordon, vous pouvez nuire à l'isolation ou dénuder le fil, et créer ainsi un risque d'incendie et de décharge électrique.
- Cessez immédiatement d'utiliser l'appareil si ce dernier se mettait à dégager de la fumée.
  Vous risqueriez sinon de provoquer un incendie ou une décharge électrique. Éteignez aussitôt l'appareil et débranchez le câble d'alimentation de la prise électrique.

2. Boîtier et voyants lumineux

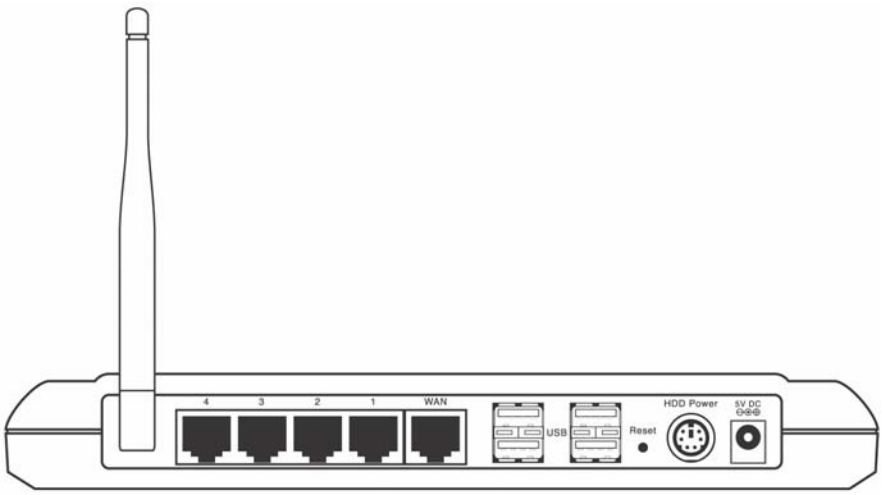
Face avant



Voyant	Couleur	État	Description
PPPoE	Rouge	Allumé	Le voyant est allumé lorsque la connexion à haut débit est de type PPPoE, Static-L2TP, DHCP-L2TP, Static-PPTP ou DHCP-PPTP. En outre, le voyant est ROUGE lorsque le serveur PPTP est activé et que la connexion PPTP est établie.
		Éteint	La connexion à haut débit n'est pas de type PPPoE.
		Clignote et voyant Status allumé	Le système d'exploitation est bloqué. La série BeWAN Secure 50 fonctionne en mode TFTP. Veuillez utiliser ce mode pour mettre à jour le firmware avec l'adresse IP par défaut 192.168.1.1.
Status	Rouge	Allumé	Mise sous tension du système en cours.
		Éteint	Le système fonctionne et la connexion est établie.
		Clignote	La configuration ou le firmware est en cours d'écriture dans la mémoire flash.
E-mail	Vert et orange		Ces deux voyants indiquent la réception d'e-mails comme décrit plus loin en détail.
WLAN (50G, M50G)		Clignote	Des données sont en cours d'émission ou de réception.
WAN Link/Act	Vert	Allumé	La liaison WAN est opérationnelle et les signaux Ethernet sont normaux.
		Éteint	La liaison WAN n'est pas opérationnelle.
		Clignote	Des données sont en cours d'émission ou de réception.
WAN 10/100M	Orange	Allumé	La vitesse de la liaison est 100 Mbps.
		Éteint	La vitesse de la liaison est 10 Mbps.
LAN Link/Act	Vert	Allumé	La liaison LAN est opérationnelle et les signaux Ethernet sont normaux.
		Éteint	La liaison LAN n'est pas opérationnelle.
		Clignote	Des données sont en cours d'émission ou de réception.

LAN 10/100M	Orange	Allumé	La vitesse de la liaison est 100 Mbps.
		Éteint	La vitesse de la liaison est 10 Mbps.

Face arrière



LAN 1-4	Port de réseau étendu (LAN). Les PC et les périphériques du réseau local sont connectés à ces ports.
WAN	Port de réseau étendu (WAN). Raccordez un modem câble ou DSL à ce port.
USB (M50, M50G)	Quatre ports USB 2.0. Ils permettent de connecter des périphériques compatibles USB 1.1/2.0 tels qu'une imprimante, une webcam, un disque dur USB, un lecteur de cartes USB, un lecteur MP3, un appareil photo numérique, etc.
Reset	Deux fonctions : 1. Pour réinitialiser le système, appuyez légèrement sur le bouton **Reset** avec un objet très pointu. 2. Pour effacer la configuration du système et restaurer la configuration d'usine, appuyez sur le bouton Reset avec un objet très pointu pendant 3 secondes jusqu'à ce que le voyant lumineux **Status** clignote. La configuration d'usine est restaurée lors du redémarrage.
HDD Power (M50, M50G)	Certains périphériques USB (généralement les disques durs externes) requièrent une alimentation supérieure à 500 mA. Si vous rencontrez des problèmes de dysfonctionnement du système lors de l'utilisation de périphériques USB, il est possible que l'alimentation ne soit pas suffisante. Raccordez le connecteur PS/2 du périphérique au port HDD Power situé à l'arrière des modèles BeWAN Secure M50 et M50G pour fournir une alimentation supplémentaire.
Power	Port 5V DC. Raccordez-y l'adaptateur secteur.

3. Installation et configuration rapide

Raccordement des BeWAN Secure série 50

Veuillez suivre les instructions ci-dessous :

Étape 1 Éteignez le PC, le modem câble/DSL et le routeur.

Étape 2 Raccordez le PC au port LAN du routeur à l'aide d'un câble Ethernet (catégorie 5 ou supérieure). Si vous disposez de plusieurs PC, répétez cette étape autant de fois que nécessaire.

Étape 3 Utilisez le câble Ethernet fourni pour raccorder le modem câble/DSL au port WAN du routeur.

Étape 4 Raccordez la sortie de l'adaptateur secteur (fiche de type casque audio) au port **Power** situé à l'arrière du routeur. Raccordez l'entrée à une prise de courant. Mettez l'appareil sous tension. Le voyant **Power** situé sur la face avant s'allume si la mise sous tension s'effectue correctement. Les BeWAN Secure série 50 effectuent ensuite un test d'autodiagnostic du système. À ce stade, le voyant **Status** est allumé. Le test d'autodiagnostic dure environ 35 secondes. Le voyant **Status** s'éteint à l'issue du processus.

Étape 5 Mettez le modem câble/DSL sous tension.

Étape 6 Mettez le PC sous tension.

Attention : si vous devez réinitialiser le routeur/restaurer la configuration d'usine, appuyez sur le bouton Reset avec un objet très pointu jusqu'à ce que le voyant Status clignote (après environ 3 secondes).

Connexion aux BeWAN Secure série 50

Après l'installation et la mise sous tension du routeur, vous pouvez commencer à configurer l'appareil. L'adresse IP par défaut de l'interface LAN du routeur est ***192.168.1.1***.

1. Lancez votre navigateur Internet (Microsoft® Internet Explorer, par exemple).
2. Dans le champ **Adresse**, saisissez l'adresse IP du routeur, puis tapez sur le touche **Entrée**. L'écran suivant devrait apparaître.

Administration BeWAN systems - Microsoft Internet Explorer
http://192.168.1.1/private/login
BeWAN systems
BeWAN Secure
Login
Webcam en directe
Résolution recommandée : 1024 x 768
Navigateurs supportés : Mozilla 1.x, FireFox 1.x, IE 6.0
Veuillez activer les cookies et le javascript dans votre navigateur
Copyright© 2005 BeWAN systems. Tous droits réservés.

3. Pour ouvrir la session, vous n'avez plus qu'à saisir le mot de passe (le mot de passe par défaut est ***bewan***). Saisissez **bewan**, puis cliquez sur le bouton **Login** ou appuyez sur la touche **Entrée** pour procéder à l'authentification du mot de passe. L'écran suivant apparaît si ce dernier est correct.

Remarque : il est impératif de tenir compte de la casse (majuscules / minuscules).

La colonne de gauche contient le menu principal et celle de droite présente les options de configuration. La langue par défaut de l'interface utilisateur est le français. Pour passer du français à l'anglais, reportez-vous au chapitre 4. Pour effectuer la configuration de base, cliquez sur **Configuration rapide** dans la colonne de gauche.

Configuration rapide

L'écran **Configuration rapide** est divisé en cinq sections : Interface WAN, Interface LAN, Mot de passe de l'administration Web, Mot de passe pour la Webcam en direct et Protocole de temps (NTP).

Interface WAN

L'interface WAN est une interface Ethernet connectée à un modem câble/DSL permettant d'accéder à Internet via un FAI (***F**ournisseur d'**A**ccès à **I**nternet*). Les FAI utilisant des structures différentes ou des applications spéciales selon la situation géographique, il existe plusieurs types de connexion. Ces derniers sont décrits ci-dessous. Veuillez contacter votre FAI local pour connaître le type de connexion à sélectionner.

Les BeWAN Secure série 50 prennent en charge les types de connexion suivants :

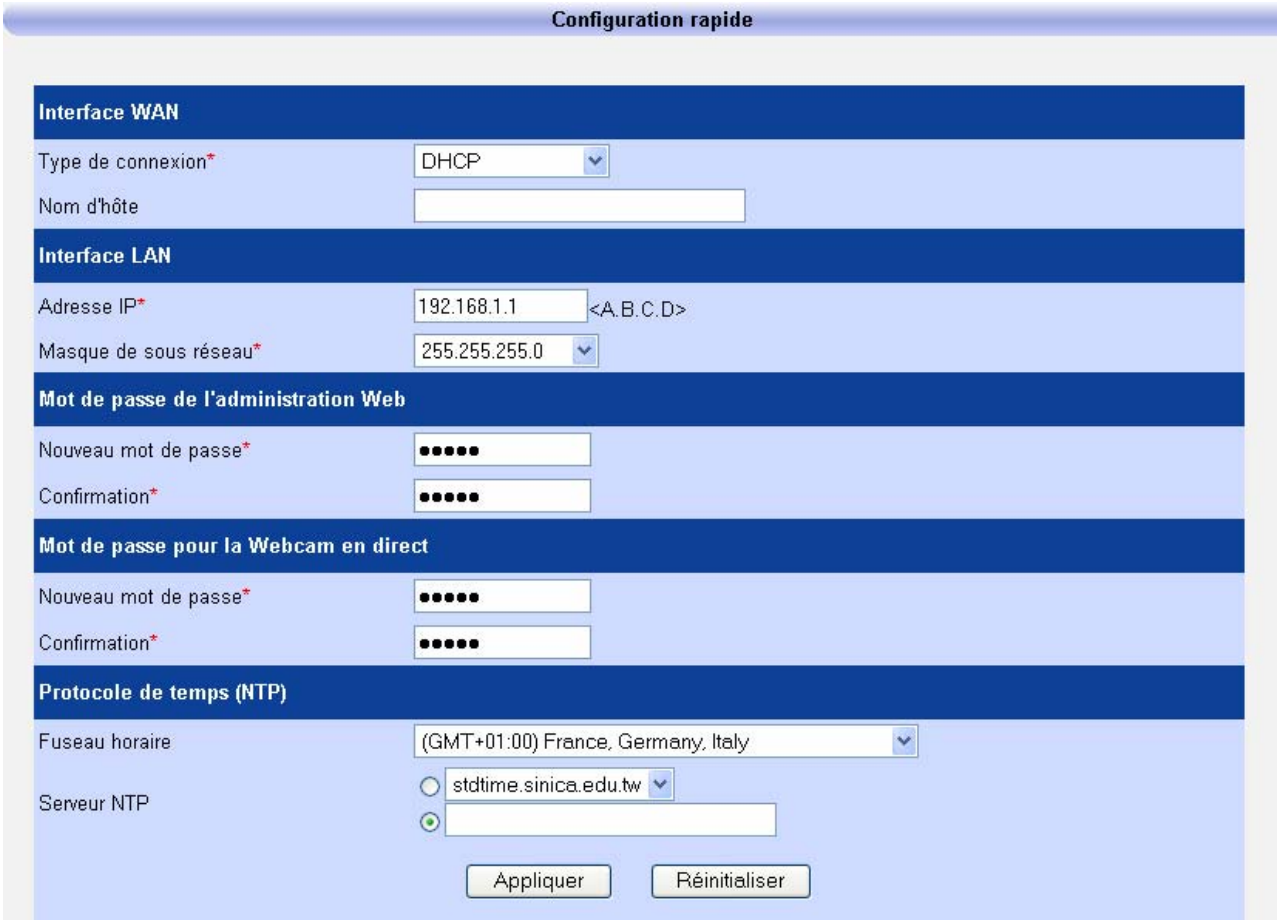
- DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol),
- Static,
- PPPoE (**P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet),
- Static-PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol),
- DHCP-PPTP,
- BIGPOND Cable,
- Static-L2TP (**L**ayer **Two T**unneling **P**rotocol),
- DHCP-L2TP.

L'état de la connexion au réseau étendu peut être affiché quel que soit le type de connexion utilisé en sélectionnant **Interfaces** > **WAN** > **Information de l'interface WAN**.

Attention : sauf avis contraire de votre FAI, veillez à ne pas modifier les valeurs PPPoE, MRU PPPoE, MTU PPPoE, Echec de l'écho LCP et Intervalle de l'écho LCP. Veuillez laisser les valeurs par défaut.

Les différents types de connexion au réseau étendu sont décrits ci-dessous :

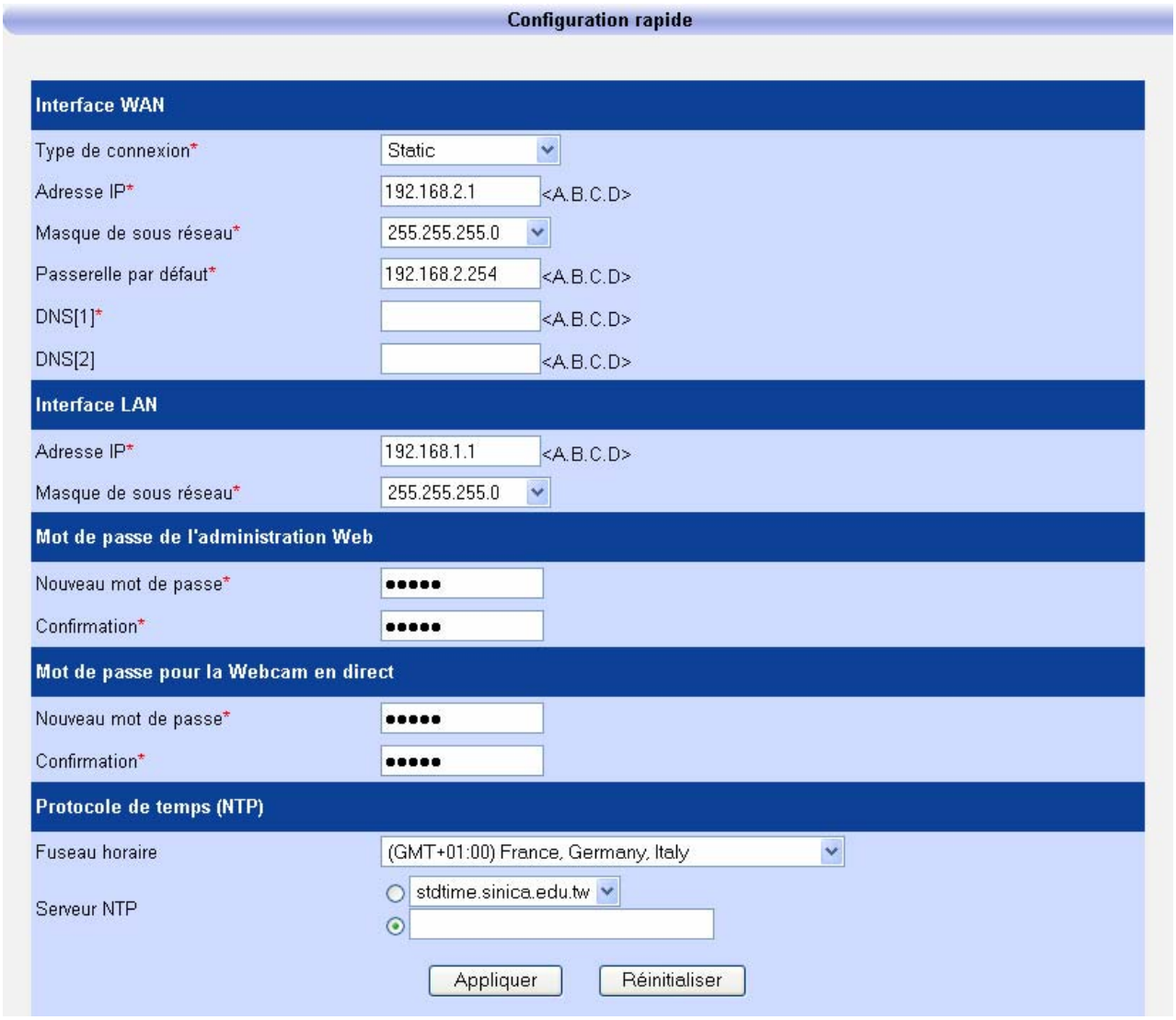
DHCP



Si votre FAI utilise une connexion de type DHCP, suivez les instructions ci-dessous.

- Sélectionnez **DHCP** dans la liste déroulante **Type de connexion**.
- Si vous utilisez un modem câble, veuillez remplacer l'adresse MAC de l'interface WAN par celle de la carte réseau fournie par votre FAI ou par celle de votre propre carte.

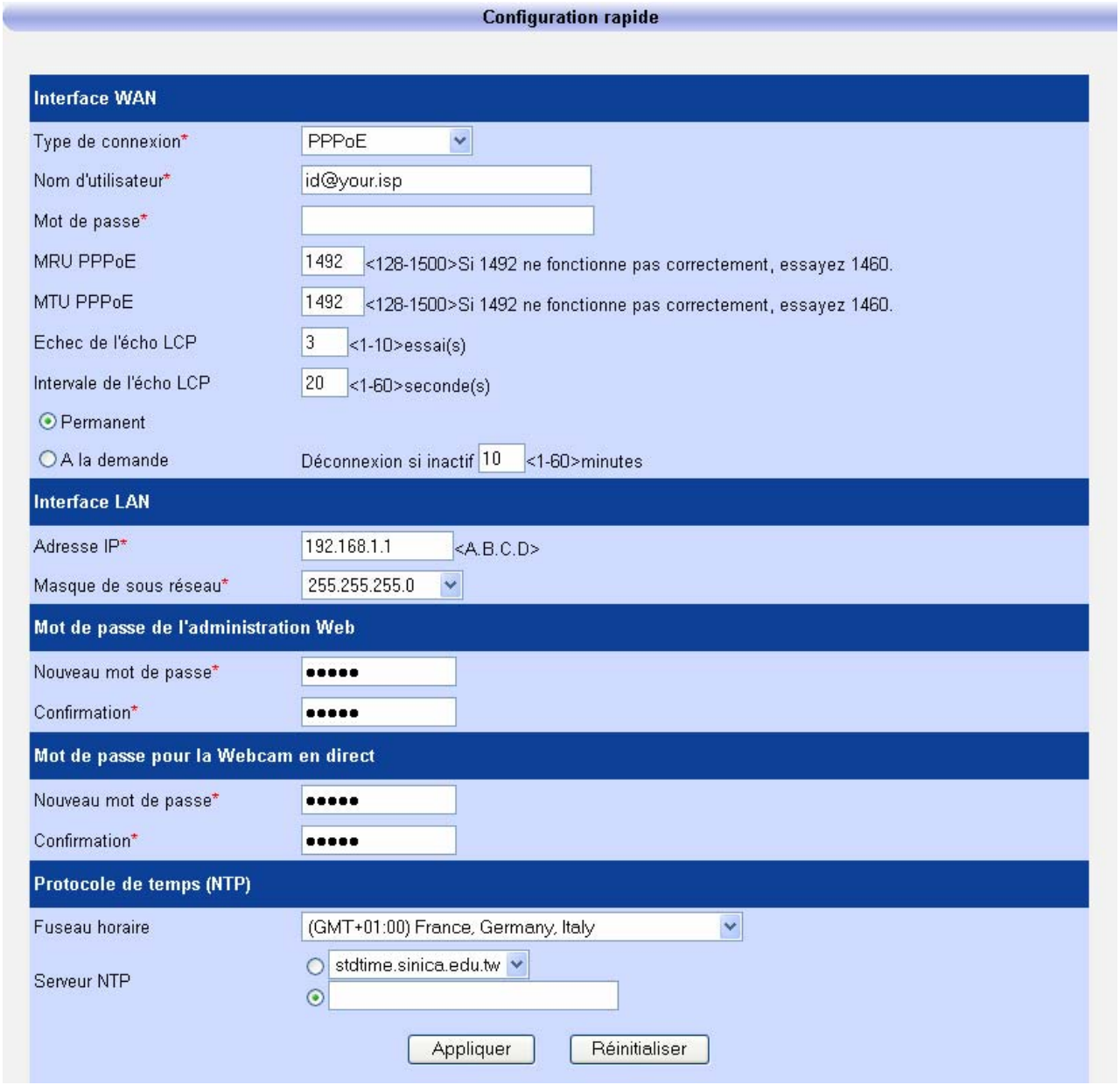
STATIC



Si votre connexion est de type Static, suivez les instructions ci-dessous :

- Sélectionnez **Static** dans la liste déroulante **Type de connexion**.
- Entrez l'adresse IP, le masque de sous-réseau et la passerelle par défaut fournis par votre FAI dans les zones de texte **Adresse IP**, **Masque de sous-réseau** et **Passerelle par défaut**.
- Saisissez au moins une adresse IP de serveur DNS fournie par votre FAI.

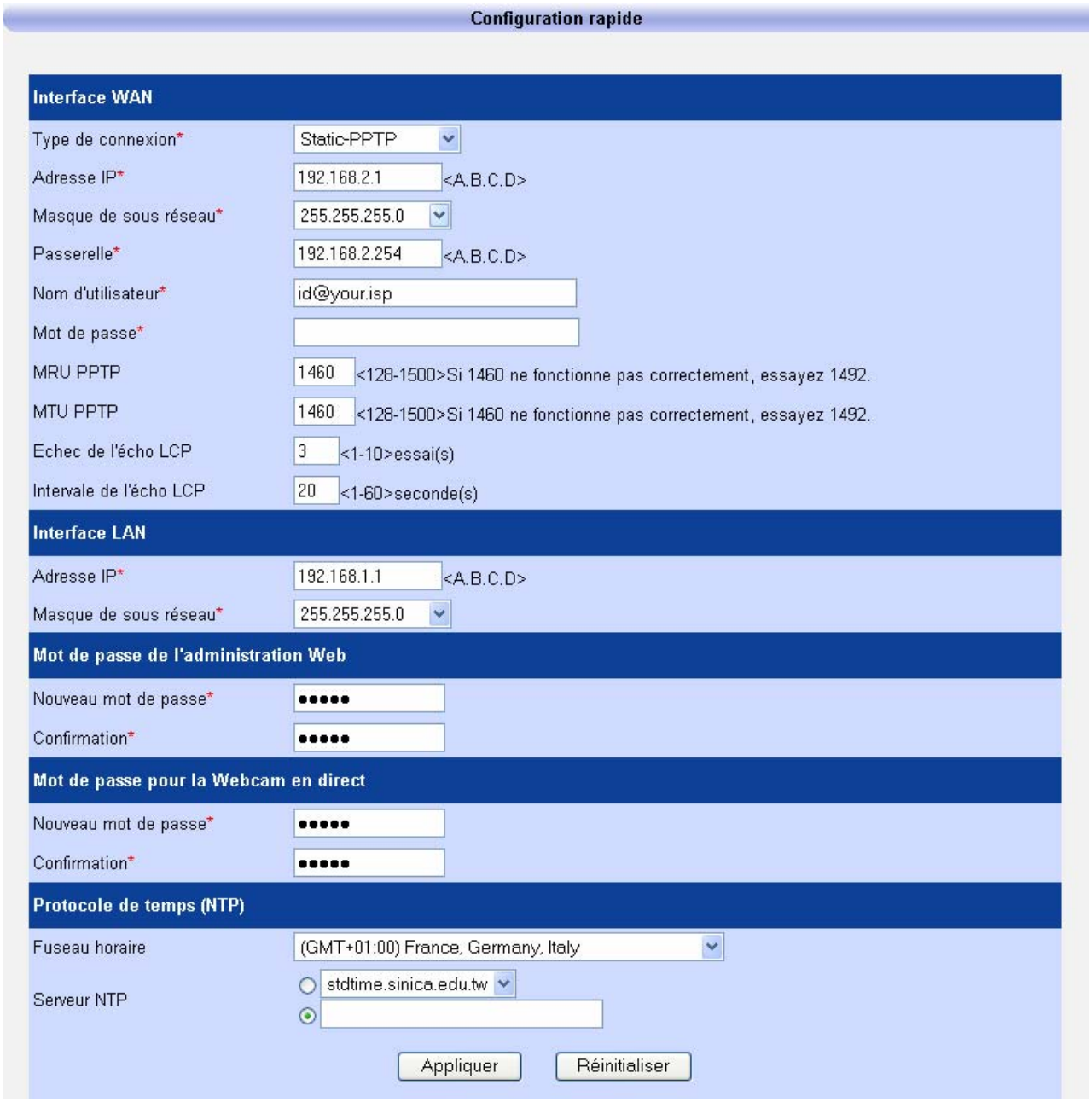
PPPoE


Configuration rapide
Interface WAN
Type de connexion* PPPoE
Nom d'utilisateur* id@your.isp
Mot de passe*
MRU PPPoE 1492 <128-1500>Si 1492 ne fonctionne pas correctement, essayez 1460.
MTU PPPoE 1492 <128-1500>Si 1492 ne fonctionne pas correctement, essayez 1460.
Echec de l'écho LCP 3 <1-10>essai(s)
Intervale de l'écho LCP 20 <1-60>seconde(s)
Permanent
A la demande Déconnexion si inactif 10 <1-60>minutes
Interface LAN
Adresse IP* 192.168.1.1 <A.B.C.D>
Masque de sous réseau* 255.255.255.0
Mot de passe de l'administration Web
Nouveau mot de passe*
Confirmation*
Mot de passe pour la Webcam en direct
Nouveau mot de passe*
Confirmation*
Protocole de temps (NTP)
Fuseau horaire (GMT+01:00) France, Germany, Italy
Serveur NTP stdtime.sinica.edu.tw
Appliquer
Réinitialiser

Si votre connexion est de type PPPoE, suivez les instructions ci-dessous :

- Sélectionnez **PPPoE** dans la liste déroulante **Type de connexion**.
- Dans la zone de texte **Nom d'utilisateur**, saisissez le nom d'utilisateur fourni par votre FAI. Certains FAI requièrent un nom d'utilisateur au format id@fai.net. Veuillez vérifier le format à utiliser auprès de votre FAI.
- Dans la zone de texte **Mot de passe**, saisissez le mot de passe correspondant.
- Vous pouvez choisir une connexion permanente ou à la demande.

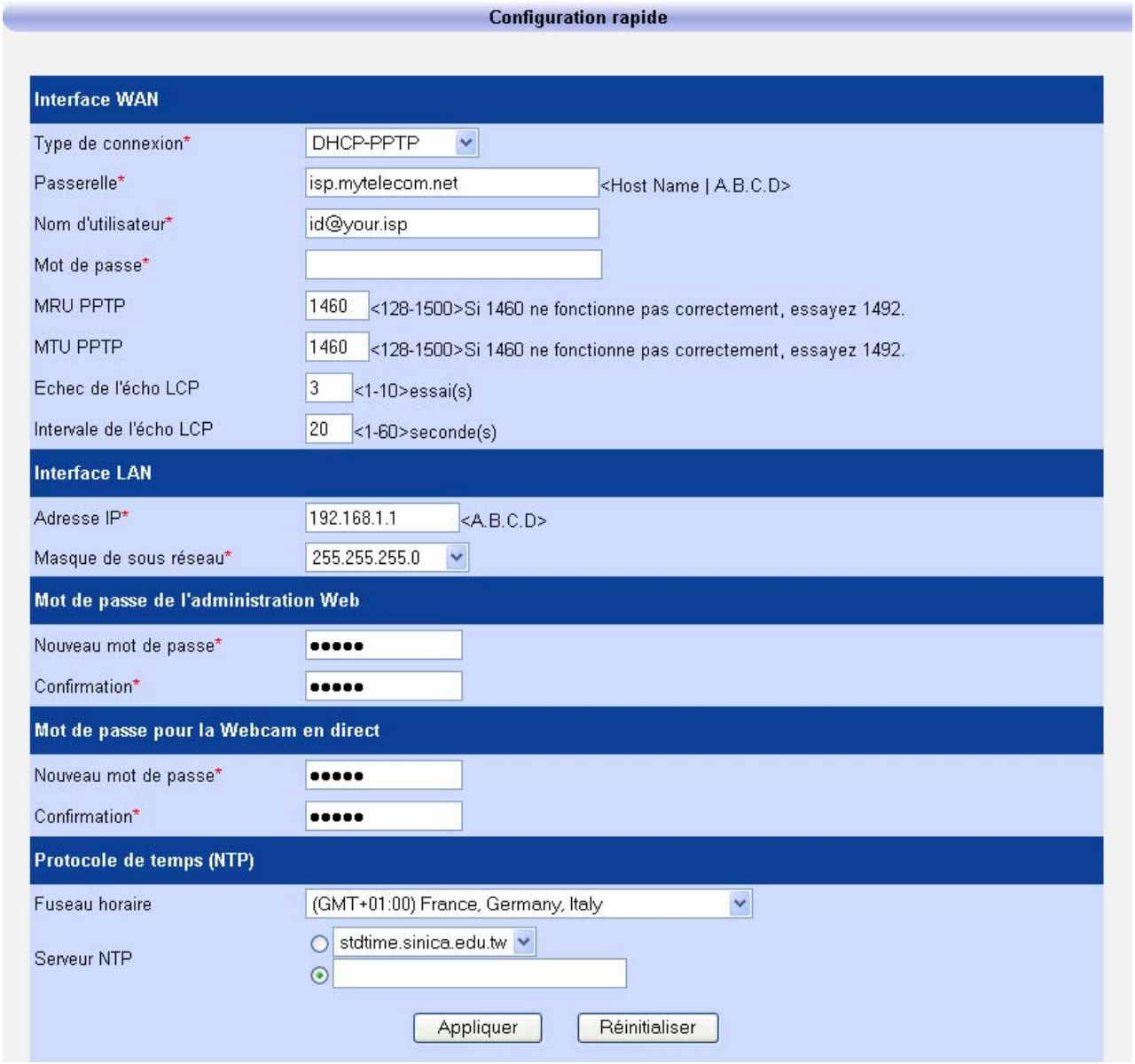
STATIC-PPTP


Configuration rapide
Interface WAN
Type de connexion* Static-PPTP
Adresse IP* 192.168.2.1 <A.B.C.D>
Masque de sous réseau* 255.255.255.0
Passerelle* 192.168.2.254 <A.B.C.D>
Nom d'utilisateur* id@your.isp
Mot de passe*
MRU PPTP 1460 <128-1500>Si 1460 ne fonctionne pas correctement, essayez 1492.
MTU PPTP 1460 <128-1500>Si 1460 ne fonctionne pas correctement, essayez 1492.
Echec de l'écho LCP 3 <1-10>essai(s)
Intervale de l'écho LCP 20 <1-60>seconde(s)
Interface LAN
Adresse IP* 192.168.1.1 <A.B.C.D>
Masque de sous réseau* 255.255.255.0
Mot de passe de l'administration Web
Nouveau mot de passe*
Confirmation*
Mot de passe pour la Webcam en direct
Nouveau mot de passe*
Confirmation*
Protocole de temps (NTP)
Fuseau horaire (GMT+01:00) France, Germany, Italy
Serveur NTP stdtime.sinica.edu.tw
Appliquer
Réinitialiser

Si vous utilisez une connexion de type Static-PPTP, suivez les instructions ci-dessous :

- Sélectionnez **Static-PPTP** dans la liste déroulante **Type de connexion**.
- Saisissez l'adresse IP, le masque de sous-réseau et la passerelle par défaut fournis par votre FAI dans les zones de texte **Adresse IP**, **Masque de sous-réseau** et **Passerelle**.
- Dans la zone de texte **Nom d'utilisateur**, saisissez le nom d'utilisateur fourni par votre FAI. Certains FAI requièrent un nom d'utilisateur au format id@fai.net. Veuillez vérifier le format à utiliser auprès de votre FAI.
- Dans la zone de texte **Mot de passe**, saisissez le mot de passe correspondant.

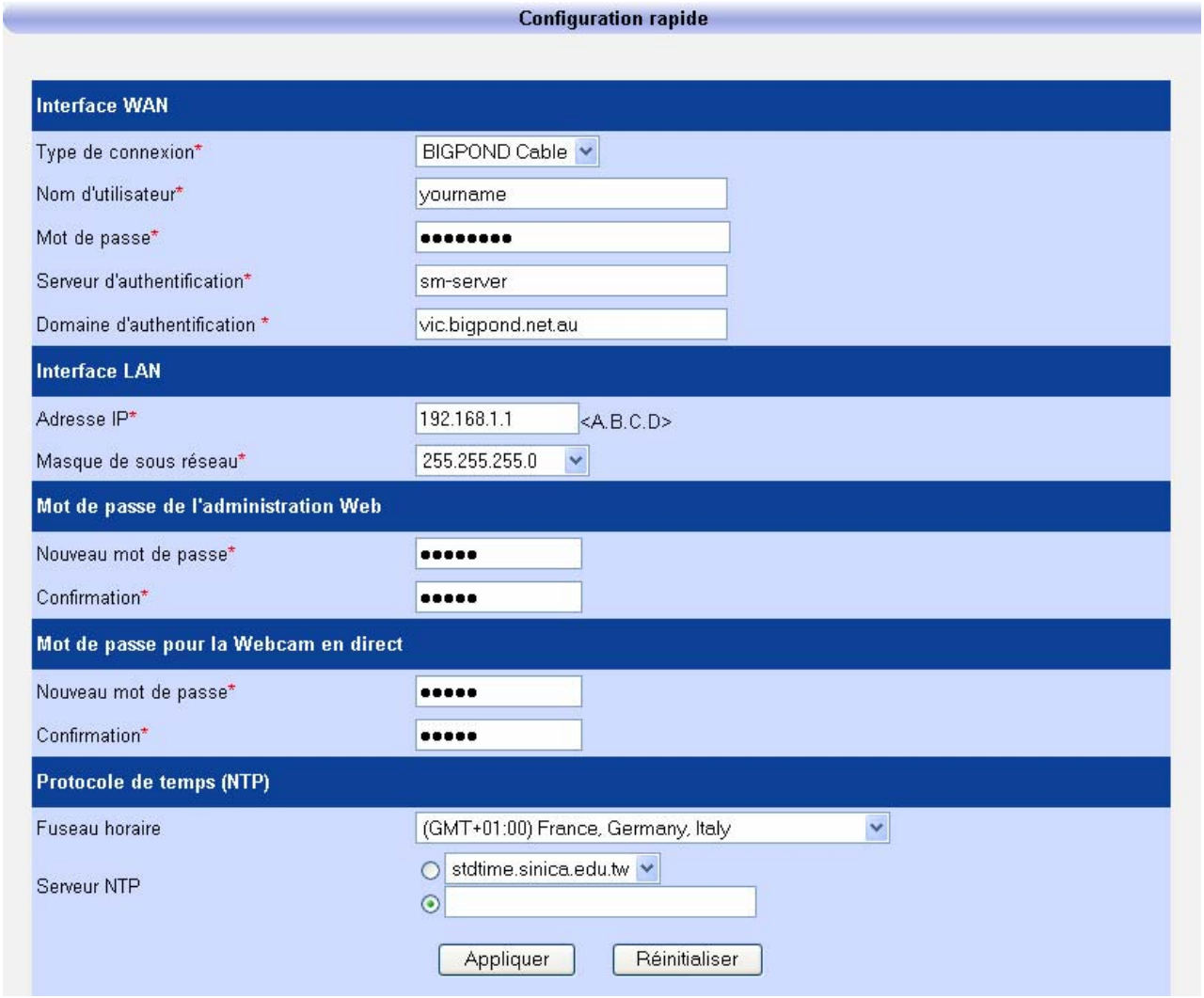
DHCP-PPTP


Configuration rapide
Interface WAN
Type de connexion* DHCP-PPTP
Passerelle* isp.mytelecom.net <Host Name | A.B.C.D>
Nom d'utilisateur* id@your.isp
Mot de passe*
MRU PPTP 1460 <128-1500>Si 1460 ne fonctionne pas correctement, essayez 1492.
MTU PPTP 1460 <128-1500>Si 1460 ne fonctionne pas correctement, essayez 1492.
Echec de l'écho LCP 3 <1-10>essai(s)
Intervale de l'écho LCP 20 <1-60>seconde(s)
Interface LAN
Adresse IP* 192.168.1.1 <A.B.C.D>
Masque de sous réseau* 255.255.255.0
Mot de passe de l'administration Web
Nouveau mot de passe*
Confirmation*
Mot de passe pour la Webcam en direct
Nouveau mot de passe*
Confirmation*
Protocole de temps (NTP)
Fuseau horaire (GMT+01:00) France, Germany, Italy
Serveur NTP stdtime.sinica.edu.tw
Appliquer
Réinitialiser

Si vous utilisez une connexion de type DHCP-PPTP, suivez les instructions ci-dessous :

- Sélectionnez **DHCP-PPTP** dans la liste déroulante **Type de connexion**.
- Dans la zone de texte **Passerelle**, saisissez le nom (par exemple, isp.mytelecom.net) ou l'adresse IP de la passerelle fourni(e) par votre FAI.
- Dans la zone de texte **Nom d'utilisateur**, saisissez le nom d'utilisateur fourni par votre FAI. Certains FAI requièrent un nom d'utilisateur au format id@fai.net. Veuillez vérifier le format à utiliser auprès de votre FAI.
- Dans la zone de texte **Mot de passe**, saisissez le mot de passe correspondant.

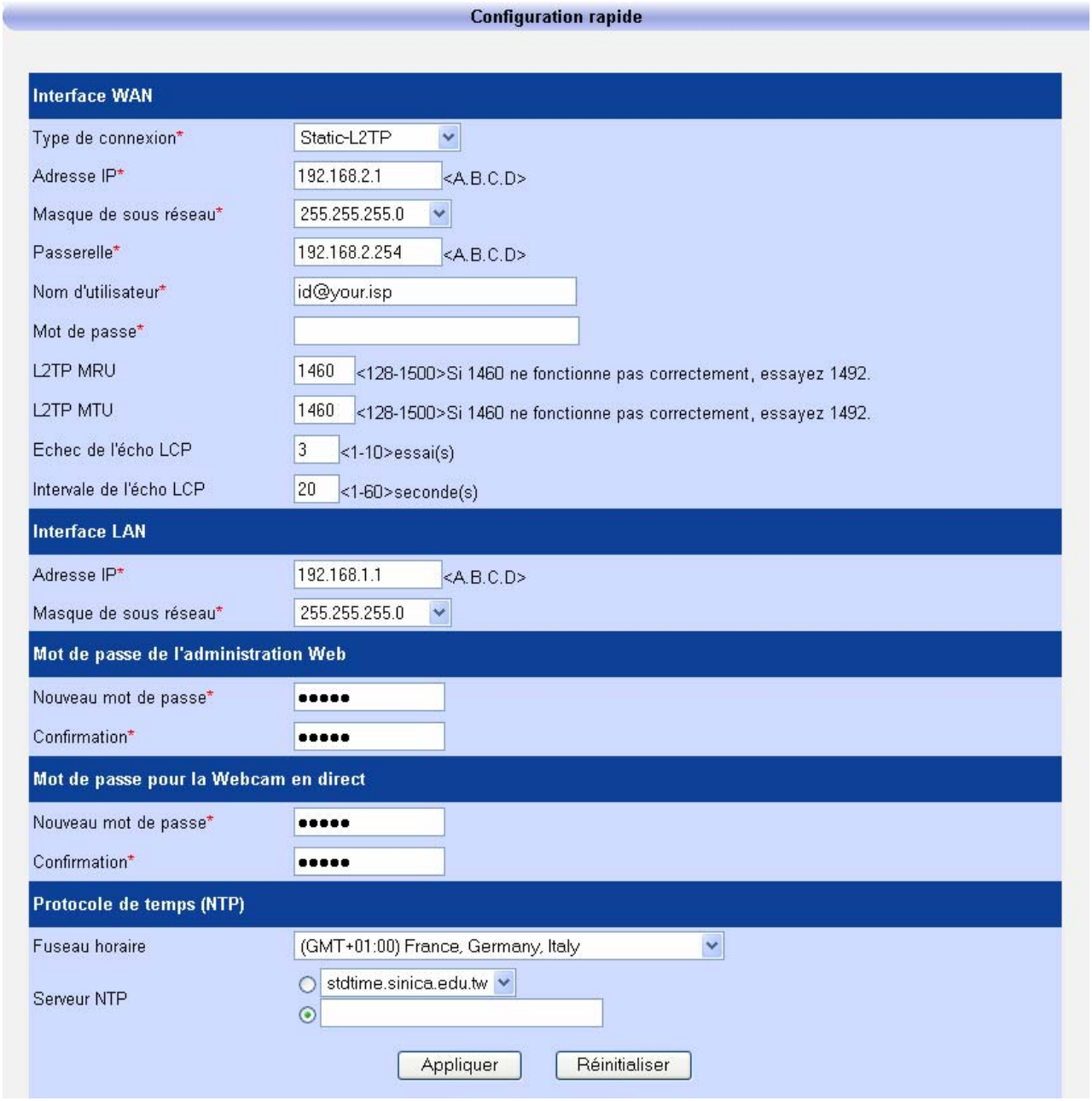
BIGPOND CABLE



Si votre connexion est de type BIGPOND Cable, suivez les instructions ci-dessous :

- Sélectionnez **BIGPOND Cable** dans la liste déroulante **Type de connexion**.
- Dans la zone de texte **Nom d'utilisateur**, saisissez le nom d'utilisateur fourni par votre FAI. Certains FAI requièrent un nom d'utilisateur au format id@fai.net. Veuillez vérifier le format à utiliser auprès de votre FAI.
- Dans la zone de texte **Mot de passe**, saisissez le mot de passe correspondant.
- Dans la zone de texte **Serveur d'authentification**, entrez le serveur fourni par votre FAI (par exemple, sm-server).
- Dans la zone de texte **Domaine d'authentification**, saisissez le nom de domaine fourni par votre FAI (par exemple, vic.bigpond.net.au).

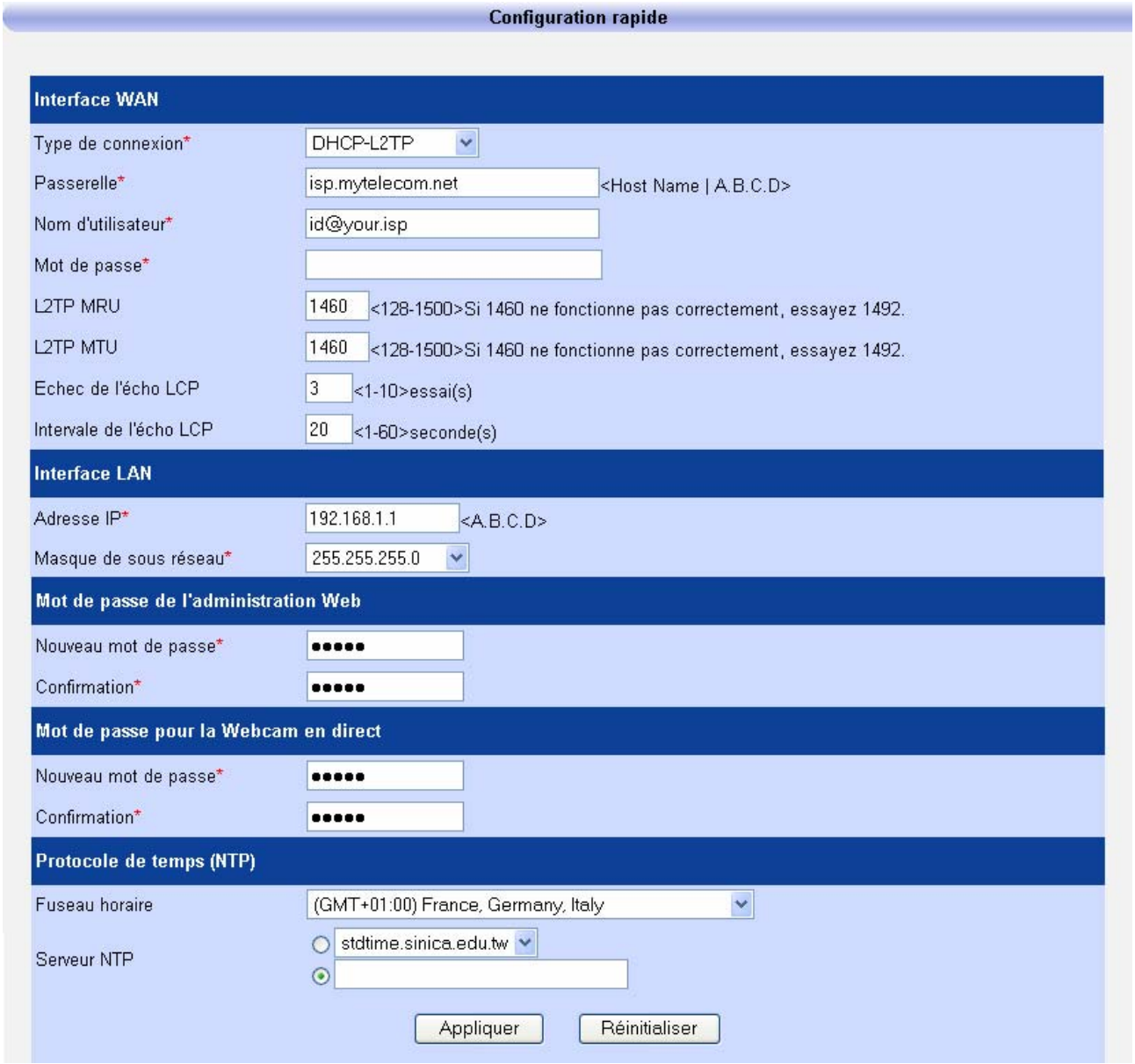
STATIC-L2TP



Si votre connexion est de type Static-L2TP, suivez les instructions ci-dessous :

- Sélectionnez **Static-L2TP** dans la liste déroulante **Type de connexion**.
- Saisissez l'adresse IP, le masque de sous réseau et la passerelle par défaut fournis par votre FAI dans les zones de texte **Adresse IP**, **Masque de sous réseau** et **Passerelle**.
- Dans la zone de texte **Nom d'utilisateur**, saisissez le nom d'utilisateur fourni par votre FAI. Certains FAI requièrent un nom d'utilisateur au format id@fai.net. Veuillez vérifier le format à utiliser auprès de votre FAI.
- Dans la zone de texte **Mot de passe**, saisissez le mot de passe correspondant.

DHCP-L2TP



Si votre connexion est de type DHCP-L2TP, suivez les instructions ci-dessous :

- Sélectionnez **DHCP-L2TP** dans la liste déroulante **Type de connexion**.
- Dans la zone de texte **Passerelle**, saisissez le nom (par exemple, isp.mytelecom.net) ou l'adresse IP de la passerelle fourni(e) par votre FAI.
- Dans la zone de texte **Nom d'utilisateur**, saisissez le nom d'utilisateur fourni par votre FAI. Certains FAI requièrent un nom d'utilisateur au format id@fai.net. Veuillez vérifier le format à utiliser auprès de votre FAI.
- Dans la zone de texte **Mot de passe**, saisissez le mot de passe correspondant.

Interface LAN

L'adresse IP et le masque de sous réseau de l'interface LAN du routeur peuvent être modifiés dans cette section. Saisissez les valeurs souhaitées dans les champs **Adresse IP** et **Masque de sous réseau**. Lorsque vous modifiez ces valeurs, veillez à modifier l'adresse IP ou le paramètre DHCP de votre PC en conséquence. Sinon, vous ne pourrez vous connecter ni à l'interface utilisateur, ni à Internet.

Mot de passe de l'administration Web

Le mot de passe utilisé pour la connexion à l'interface utilisateur peut être modifié dans cette section.

Pour des raisons évidentes de sécurité, nous vous recommandons vivement de changer le mot de passe d'administration.

Saisissez le nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmation**. Le nouveau mot de passe prendra effet à la prochaine connexion.

Protocole de temps (NTP)

Fuseau horaire Sélectionnez votre fuseau horaire.

Serveur NTP Saisissez l'adresse IP du serveur NTP dans ce champ.

Cliquez sur **Appliquer** pour que les nouveaux paramètres soient pris en compte et pour activer la liaison WAN.

Si votre connexion est de type PPPoE, le voyant PPPoE (en face avant) s'allume dès que la connexion à Internet est établie. Pour vérifier l'état de la liaison ou les informations IP, sélectionnez **Interfaces** > **WAN** > **Information de l'interface WAN**.

Si tous les paramètres de configuration sont corrects, il est recommandé de les sauvegarder en cliquant sur l'icône **Sauvegarder** dans le coin supérieur droit de la fenêtre. Ils seront ainsi stockés dans la mémoire flash.

Attention : les paramètres modifiés seront perdus à la prochaine connexion si vous ne les sauvegardez pas avant de mettre l'appareil hors tension.

4. Administration Web

L'administration Web offre une interface simple à utiliser pour la configuration et la maintenance du système.

La colonne de gauche contient le menu principal, celle de droite présente les options de configuration. La configuration du système et les informations concernant ce dernier peuvent être consultées à partir du menu arborescent. Le menu principal est divisé en plusieurs sections :

- Configuration rapide
- Interfaces
    - ✓ LAN
    - ✓ WAN
    - ✓ Wireless (modèles BeWAN Secure M50 et M50G)
- Filtrage de contenu
    - ✓ Filtrage de mots clés
    - ✓ Blocage d'URL
    - ✓ IP autorisées
    - ✓ Ports filtrés
- Réglages avancés
    - ✓ DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol)
    - ✓ DNS (**D**omain **N**ame **S**ystem) dynamique
    - ✓ Mappage des ports
    - ✓ Pare-feu
    - ✓ Serveur virtuel
    - ✓ Gestion de la bande passante
    - ✓ VPN (**V**irtual **P**rivate **N**etwork)
    - ✓ SIP
    - ✓ Routes statiques
    - ✓ ARP
    - ✓ Table des noms d'hôte
    - ✓ Wake On LAN
    - ✓ VLAN
- Surveillance des emails
    - ✓ Groupes de mail
    - ✓ Serveurs de mails

- Webcam (modèles BeWAN Secure M50 et M50G)
    - ✓ Réglage
    - ✓ Planification de détection
    - ✓ Alerte par Email
    - ✓ Webcam en direct
- Serveur FTP (modèles BeWAN Secure M50 et M50G)
    - ✓ Compte FTP
    - ✓ Paramètres FTP
    - ✓ État du serveur FTP
- Maintenance
    - ✓ Administration système
    - ✓ Information système
    - ✓ Langue
    - ✓ Heure
    - ✓ Périphériques USB (modèles BeWAN Secure M50 et M50G)
    - ✓ Utilisateurs en ligne
    - ✓ Firmware & Configuration
    - ✓ Ping
    - ✓ Traceroute
    - ✓ Log
- Icône Redémarrer
- Icône Sauvegarder
- Icône Déconnecter

Remarque : lorsque vous saisissez ou sélectionnez de nouvelles valeurs dans l'interface d'administration Web, vous devez cliquer sur le bouton ***Appliquer*** *correspondant pour que les modifications soient prises en compte.*

Dans l'administration Web, s'il est indiqué que vous devez entrer <**A.B.C.D**>, cela signifie que vous devez saisir l'adresse IP d'un seul hôte, comme par exemple 192.168.1.30 ; s'il est indiqué que vous devez entrer <**A.B.C.D/M**>, cela signifie que vous devez saisir un sous réseau, M représentant la largeur du masque de sous réseau en bits. Par exemple, 192.168.1.0/24 équivaut à 192.168.1.0 avec un masque de sous réseau de 24 bits (255.255.255.0). S'il est indiqué que vous devez entrer <**A.B.C.D[/M]**>, cela signifie que vous pouvez saisir l'adresse IP d'un seul hôte ou le sous réseau.

Remarque : les modifications ne sont prises en compte que lorsque vous cliquez sur le bouton ***Appliquer*** *dans l'interface utilisateur.*

Tous les paramètres de configuration sont décrits dans les chapitres suivants.

Configuration rapide

Veuillez vous reporter au chapitre 3, « Installation et configuration rapide ».

Interfaces

Le menu **Interfaces** comporte trois sections : LAN, WAN et Wireless. Si vous avez effectué la **Configuration rapide**, vous n'avez pas à configurer les interfaces LAN et WAN dans cette section.

Interface LAN

Adresse IP

Saisissez l'adresse IP du routeur. Ce champ devrait déjà contenir la valeur ***192.168.1.1***.

Masque de sous-réseau

Entrez le masque de sous-réseau. Ce champ devrait déjà contenir une valeur. La valeur par défaut est ***255.255.255.0***.

Interface WAN

MAC

MAC (***M**edia **A**ccess **C**ontrol*) : contrôle d'accès au support. L'adresse MAC est l'adresse physique de la carte Ethernet. Si vous utilisez un modem câble, veuillez remplacer l'adresse MAC de l'interface WAN par celle de la carte réseau fournie par votre FAI ou par celle de votre propre carte.

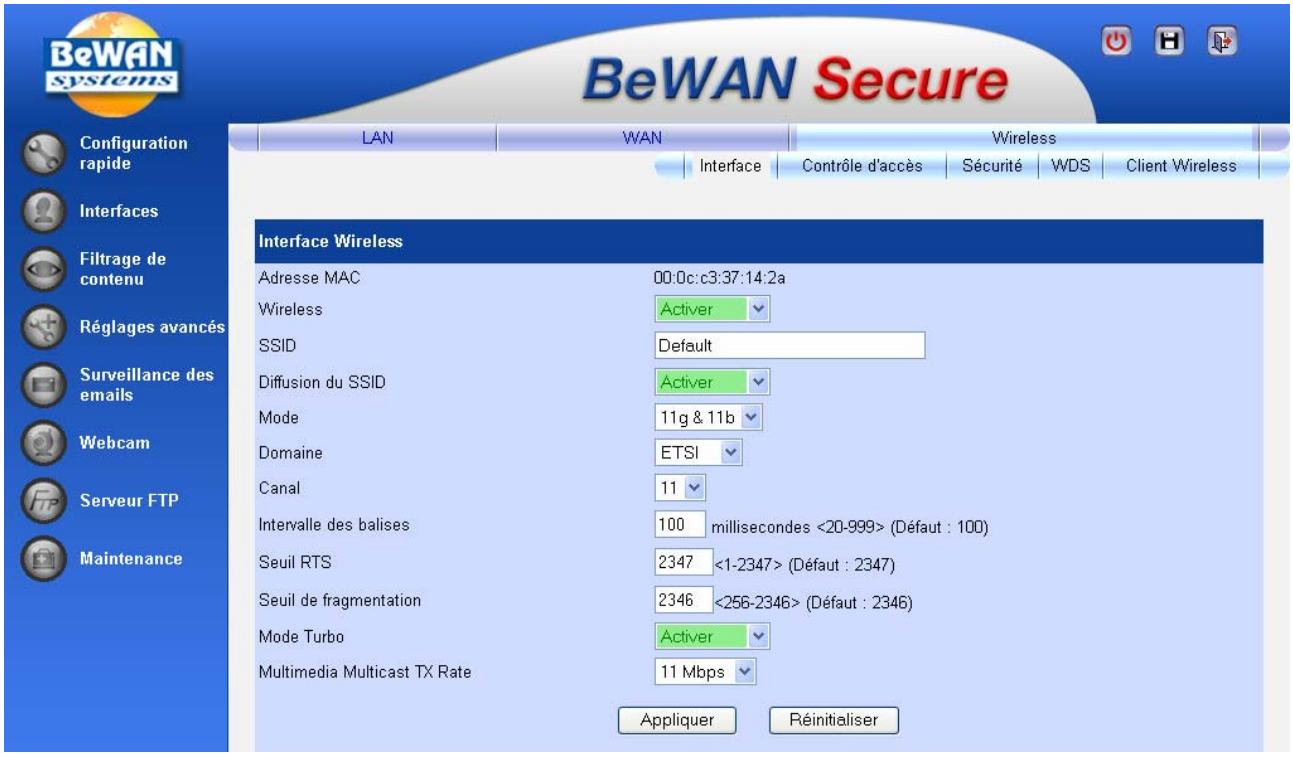
MTU

MTU (***M**aximum **T**ransmission **U**nit*) : unité de transmission maximale. La taille MTU est la dimension maximale des paquets IP pouvant être autorisée en émission sans fragmentation. Ce paramètre est généralement défini sur 576 ou 1500. Il est recommandé de le définir par défaut sur 1500. Selon le fournisseur d'accès Internet auprès duquel vous avez souscrit un abonnement, vous pouvez avoir besoin de diminuer la taille de ce paramètre. Cette modification ne doit être réalisée que si la connexion de votre FAI le requiert.

Veuillez vous reporter au chapitre 3, « Installation et configuration rapide », pour en savoir plus sur l'interface WAN.

Interface Wireless (modèles BeWAN Secure 50G et M50G)

Vous pouvez configurer les paramètres de la connexion sans fil dans cette section.



Wireless

Permet d'activer ou de désactiver l'option sans fil.

SSID (Service Set Identifier)

Le SSID est une chaîne d'identification pouvant comporter jusqu'à 32 caractères ASCII et permettant de différencier les différents points d'accès. Choisissez vos caractères entre "a-z", "A-Z" et "0-9".

Vous pouvez utiliser le SSID par défaut (***Default***) ou en créer un. Si plusieurs points d'accès sans fil sont disponibles dans la zone, le SSID et le canal du BeWAN Secure 50G/M50G doivent être différents de ceux des autres points d'accès. En outre, tout périphérique (PDA, ordinateur portable, etc.) souhaitant communiquer avec le BeWAN Secure 50G/M50G doit avoir le même SSID que ce dernier. Pour une raison de sécurité, nous vous conseillons de changer ce SSID lors de l'installation du routeur. Il est sensible à la casse.

Diffusion du SSID

Permet d'activer ou de désactiver la fonction de diffusion du SSID du BeWAN Secure 50G/M50G sur le réseau sans fil. Comme indiqué plus haut, pour qu'un client puisse communiquer avec le BeWAN Secure 50G/M50G, il doit avoir le même SSID que ce dernier.

Si la diffusion du SSID est activée, le client peut détecter le réseau sans fil. Si elle n'est pas activée, les clients recherchant des connexions sans fil ne peuvent pas détecter le BeWAN Secure 50G/M50G. Le seul moyen de permettre au client d'accéder à Internet via le routeur est d'entrer le même SSID que celui du système.

Mode

Le BeWAN Secure 50G/M50G est compatible avec les normes 802.11g et 802.11b. La valeur par défaut est **11g & 11b**. Cela signifie que le système peut communiquer avec les clients utilisant la norme 802.11g et/ou 802.11b.

Domaine

Le domaine diffère selon la situation géographique. Il détermine le numéro de canal pris en charge dans l'option suivante.

Canal

Les normes IEEE 802.11g et 802.11b utilisent l'étalement de spectre à séquence directe (DSS). Cette technique divise le flux d'informations à transmettre en petits paquets, chacun d'eux étant affecté aux différentes fréquences d'un canal du spectre. Comme indiqué plus haut, pour que le client et le BeWAN Secure 50G/M50G puissent communiquer entre eux, ils doivent utiliser le même SSID et le même canal. Les clients peuvent choisir le canal dans la liste des réseaux disponibles. Si le SSID doit être saisi manuellement, veillez à ce que le canal affecté au niveau du client soit identique à celui du BeWAN Secure 50G/M50G. En d'autres termes, le routeur et le client doivent utiliser le même SSID et le même canal pour pouvoir communiquer.

Intervalle des balises

Il s'agit du signal envoyé périodiquement par le point d'accès sans fil pour synchroniser les différentes stations du réseau sans fil. Laissez la valeur par défaut.

Seuil RTS

Quand le réseau Ethernet sans fil transmet des paquets de diffusion, de multidiffusion ou de monodiffusion, il les transmet directement. Toutefois, s'il doit transmettre un paquet de monodiffusion volumineux, le délai de transmission étant plus long, il envoie un paquet RTS (***R**equest **T**o **S**end*) pour demander une période de monopolisation afin d'éviter qu'il ne soit corrompu à cause d'une collision avec les paquets des autres stations. Durant cette période, les autres périphériques appartenant au même réseau sans fil cesseront d'envoyer des paquets. Par conséquent, ce seuil doit être défini selon les cas. Lorsqu'il y a beaucoup d'utilisateurs dans la zone couverte par le réseau sans fil, un seuil de demande de transmission bas peut réduire le risque de collision mais aura plutôt pour effet de réduire l'efficacité de la transmission de l'ensemble du réseau sans fil ; lorsqu'il y a peu d'utilisateurs, augmenter le seuil de demande de transmission peut améliorer l'efficacité globale de la transmission du réseau sans fil.

Seuil de fragmentation

Ce champ est utilisé pour préciser le seuil de fragmentation au-dessus duquel les paquets seront fragmentés. La fragmentation permet de découper un paquet IP en une série de plus petits fragments. Si la longueur de la trame de données transmise est supérieure au seuil de fragmentation, la trame de données sera fragmentée. Si votre réseau sans fil est soumis à des interférences importantes ou fait l'objet d'une utilisation intensive, une valeur de fragmentation peu élevée peut accroître la fiabilité de la transmission mais compromettre son efficacité. Il est préférable de définir un seuil de fragmentation plus élevé.

Mode Turbo

Le mode Turbo est spécifique à la norme 802.11g. La technique d'envoi de trames en rafale (Frame Bursting) est utilisée pour réduire le temps d'attente. Les paquets sont transmis plus rapidement. Le client doit prendre en charge le mode Turbo pour que cette technique fonctionne.

CONTROLE D'ACCES

Par défaut, tout ordinateur sans fil configuré avec le SSID et le numéro de canal du réseau peut se connecter au BeWAN Secure 50G et M50G.

Afin d'accroître la sécurité du réseau sans fil, en plus du mécanisme de cryptage (reportez-vous à la section « Sécurité » page 30), les routeurs BeWAN Secure 50G et M50G gèrent une table des adresses MAC. Vous pouvez ainsi créer l'une des listes suivantes :

- une liste noire : les ordinateurs sans fil figurant dans cette liste **ne peuvent pas** accéder au BeWAN Secure 50G et M50G, mais tous les autres ordinateurs sans fil **peuvent** s'y connecter.
- une liste blanche : les ordinateurs sans fil figurant dans cette liste **peuvent** accéder au BeWAN Secure 50G et M50G, mais tous les autres ordinateurs sans fil **ne peuvent pas** s'y connecter.

L'adresse MAC est l'identifiant physique du matériel. Cette adresse est unique. Bien que cette solution soit lourde à gérer pour peu que l'on dispose de nombreux matériels à saisir, elle permet de limiter les risques d'intrusion.

Pour configurer le contrôle d'accès au routeur et pour indiquer quels ordinateurs sans fil peuvent accéder au routeur, sélectionnez l'une des options suivantes :

- Si vous désirez que tous les ordinateurs sans fil puissent accéder au BeWAN Secure 50G et M50G, dans la rubrique **Règle**, sélectionnez l'option **Tout**.
- Si vous souhaitez créer une liste noire des ordinateurs ne pouvant pas accéder au BeWAN Secure 50G et M50G, dans la **Table MAC**, indiquez tout d'abord l'**Adresse MAC** du client Wi-Fi non autorisé à accéder au routeur, puis cliquez sur **Ajouter**. Renouvelez cette opération pour chaque client Wi-Fi. Les adresses spécifiées s'ajoutent au fur et à mesure à la table MAC affichée à l'écran.

  Dans la rubrique **Règle**, sélectionnez ensuite l'option **Refuser**.
- Si vous souhaitez créer une liste blanche des ordinateurs pouvant accéder au BeWAN Secure 50G et M50G, dans la **Table MAC**, indiquez tout d'abord l'**Adresse MAC** du client Wi-Fi autorisé à accéder au routeur, puis cliquez sur **Ajouter**. Renouvelez cette opération pour chaque client Wi-Fi. Les adresses spécifiées s'ajoutent au fur et à mesure à la table MAC affichée à l'écran.

  Dans la rubrique **Règle**, sélectionnez ensuite l'option **Accepter**.

*Remarque : l'action **Accepter** ou **Refuser** s'applique à toutes les adresses MAC que vous ajoutez. Si vous souhaitez ensuite supprimer une adresse MAC, sélectionnez-la dans la liste, puis cliquez sur le bouton **Supprimer**.*

SECURITE

Lorsque vous avez déterminé une valeur d'identification et un canal de transmission, l'un des aspects majeurs du réseau sans fil est la sécurité. C'est pourquoi le BeWAN Secure 50G/M50G prévoit des mécanismes d'authentification, un mode de cryptage afin de sécuriser les données entre la station et le point d'accès. En effet, sans cryptage, n'importe qui dans la zone de couverture du réseau peut intercepter et décoder les trames qui ne lui sont pas destinées.

Sélectionnez votre méthode de sécurité. Le routeur propose 3 types de sécurité. Les utilisateurs ont le choix entre **Aucun**, **WEP** et **WPA-PSK**.

Par défaut, l'option **Aucun** est sélectionnée.

WEP

Le WEP (***W**ired **E**quivalent **P**rivacy*) est un mécanisme d'authentification des utilisateurs. Vous sécurisez la transmission des données entre le routeur et une station cliente ou entre deux Points d'Accès au moyen d'une clé de cryptage. En effet, sans cryptage, n'importe qui dans la zone de couverture du réseau peut intercepter et décoder les trames qui ne lui sont pas destinées.

La clé WEP est statique. Pour la modifier, il faut une intervention manuelle.

Sélectionnez le niveau d'encryptage (correspondant à la longueur de la clé). Nous vous conseillons d'utiliser le niveau d'encryptage le plus élevé.

Si vous sélectionnez le mode ***ASCII***, choisissez vos caractères entre "a-z", "A-Z" et "0-9".

En revanche, si vous sélectionnez le mode ***Hexadécimal***, vos caractères doivent être compris entre "a-f", "A-F" et "0-9".

Utilisation des clés

- 64bit WEP key (HEX) : saisissez 10 chiffres hexadécimaux.
- 128bit WEP key (HEX) : saisissez 26 chiffres hexadécimaux.
- 64bit WEP key (ASCII) : saisissez 5 chiffres ASCII.
- 128bit WEP key (ASCII) : saisissez 13 chiffres ASCII.

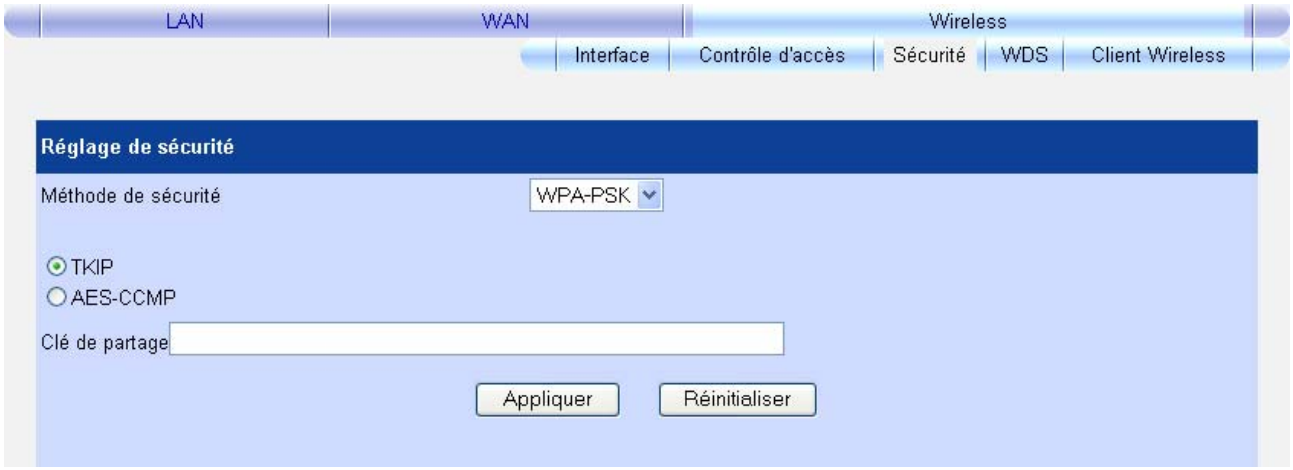
Exemple du format d'une clé WEP **64bit** en mode ***ASCII*** ou en mode ***Hexadécimal*** :

- En ASCII : *MaCle*
- En Hexadécimal : *11AA22BB33*

L'important est de noter très soigneusement le résultat obtenu pour pouvoir ensuite configurer vos stations clientes ou un autre Point d'Accès. Activez alors le WEP sur chacun de vos équipements Wireless, puis reportez la clé du routeur que vous avez saisie, et la liaison se rétablira entre vos équipements Wireless et le BeWAN Secure 50G/M50G (en effet, lorsque vous avez activé le cryptage WEP sur le routeur, la liaison s'est logiquement rompue avec les autres équipements composant votre réseau sans fil...).

WPA-PSK

Le WPA (***Wi-Fi Protected Access***) est un protocole de sécurité destiné à remplacer l'actuel WEP (***Wired Equivalent Privacy***) pour les liaisons Wi-Fi, lequel utilise des clés statiques qu'il faut changer manuellement.



Le WPA utilise différents protocoles de cryptage des données (ou algorithmes) :

- TKIP (***Temporal Key Integrity Protocol***) : l'option **TKIP** est sélectionnée par défaut. Au lieu d'utiliser une clé fixe pour chiffrer les paquets de données, il génère régulièrement de nouvelles clés dynamiques dérivées de la clé principale, permettant ainsi une sécurité accrue.

  Remarque : tous les appareils existants peuvent en bénéficier en effectuant une simple mise à jour logicielle.

- AES (***A**dvanced **E**ncryption **S**tandard*), appelé aussi WPA2 : c'est un algorithme de type symétrique et de chiffrement par blocs. Ce cryptage par blocs permet une meilleure sécurité.

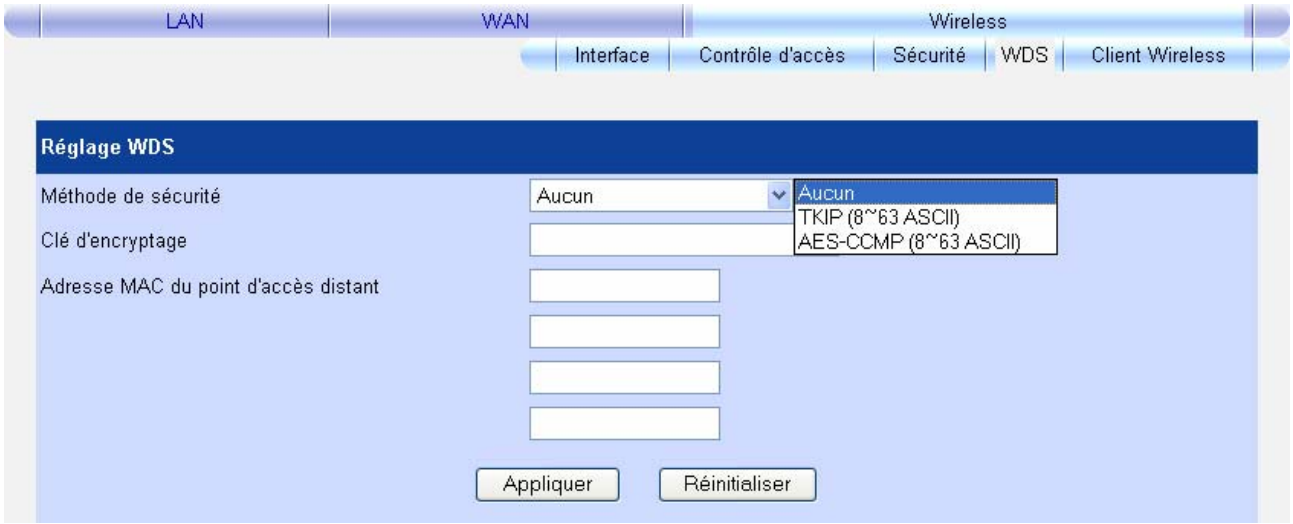
  Attention : cela nécessite l'utilisation d'une puce dédiée. Impossible donc de mettre à jour un matériel déjà existant. Sa compatibilité reste limitée au matériel équipé de cette puce.

Dans la rubrique **Clé de partage**, saisissez la valeur de votre clé. Cette clé doit comporter entre 8 et 63 caractères.

Remarque : pour la configuration des postes clients en WPA, veuillez vous reportez à la documentation fournie avec votre matériel.

WDS

Le réglage WDS (***W**ireless **D**istribution **S**ystem*) permet aux points d'accès de communiquer entre eux. Pour que le point d'accès 1 puisse communiquer avec le point d'accès 2, certains paramètres doivent être configurés. Les communications entre les points d'accès augmentent la portée du réseau sans fil.



Méthode de sécurité

Le BeWAN Secure 50G/M50G prend en charge le cryptage WPA.

Clé d'encryptage

Pour saisir votre clé, reportez-vous à la section précédente « Sécurité ».

Adresse MAC du point d'accès distant

Saisissez l'adresse MAC du point d'accès distant auquel vous souhaitez vous connecter.

Filtrage de contenu

Quatre fonctions sont proposées pour le Filtrage de contenu : Filtrage de mots clés, Blocage d'URL, IP autorisées et Ports filtrés.

Filtrage de mots clés

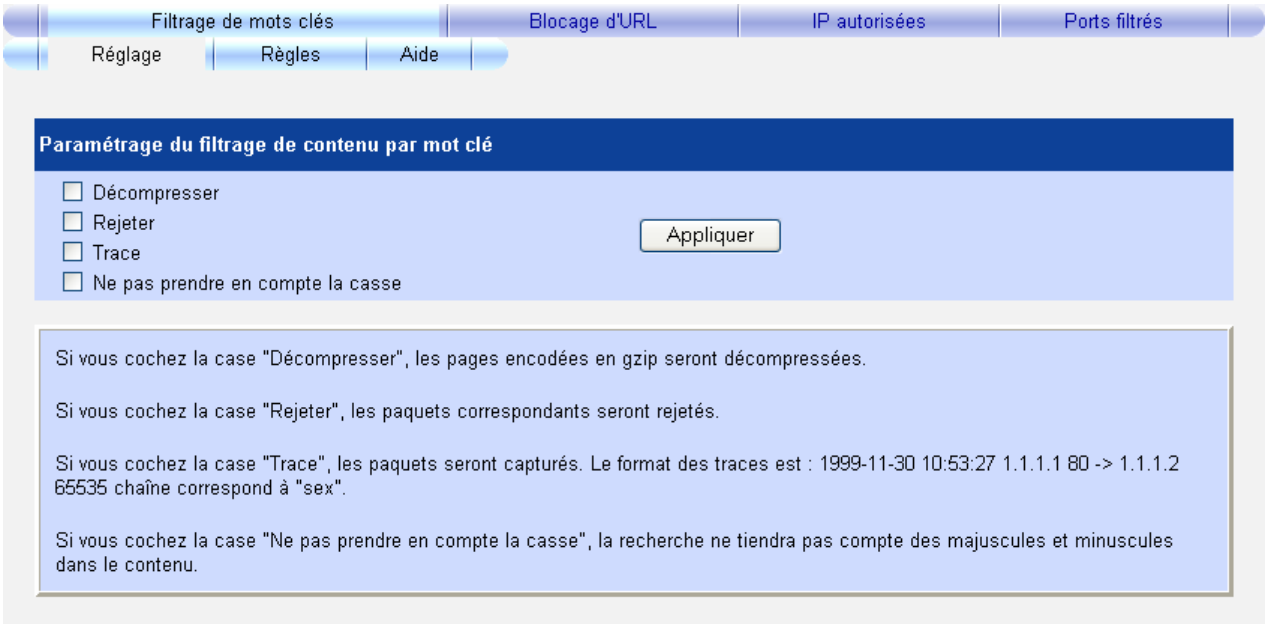
REGLES

Les utilisateurs peuvent définir certains mots clés à filtrer.

Filtrage de mots clés
Blocage d'URL
IP autorisées
Ports filtrés
Réglage
Règles
Aide
Expression / Mot clé régulier
Opération
Ajouter
Si vous indiquez "sex" comme mot clé, ce contenu sera recherché (ex. : sex, sexy, sexangle...). Si vous voulez filtrer uniquement le mot "sex" , indiquez " sex " avec des espaces avant et après. Vous pouvez aussi indiquer des mots encodés en BIG-5, UTF-8, GB ... Pour cela, veuillez changer le type d'encodage des caractères dans votre navigateur.

Vous pouvez soit les saisir directement, soit utiliser les expressions usuelles pour les désigner. En outre, les mots clés peuvent être en anglais, en français et en toute autre langue prise en charge par votre navigateur. Après avoir saisi un mot clé, cliquez sur le bouton **Ajouter** pour qu'il soit pris en compte. Pour supprimer un mot clé, cochez la case correspondante et cliquez sur **Supprimer**.

REGLAGE


Filtrage de mots clés
Blocage d'URL
IP autorisées
Ports filtrés
Réglage
Règles
Aide
Paramétrage du filtrage de contenu par mot clé
Décompresser
Rejeter
Trace
Ne pas prendre en compte la casse
Appliquer
Si vous cochez la case "Décompresser", les pages encodées en gzip seront décompressées.
Si vous cochez la case "Rejeter", les paquets correspondants seront rejetés.
Si vous cochez la case "Trace", les paquets seront capturés. Le format des traces est : 1999-11-30 10:53:27 1.1.1.1 80 -> 1.1.1.2 65535 chaîne correspond à "sex".
Si vous cochez la case "Ne pas prendre en compte la casse", la recherche ne tiendra pas compte des majuscules et minuscules dans le contenu.

Décompresser

Certains contenus Web sont compressés. Pour pouvoir filtrer le contenu compressé, le système doit le décompresser. Cochez ou non cette option en fonction de vos besoins.

Rejeter

Si vous cochez l'option **Rejeter**, les pages Web contenant le mot clé associé seront rejetées par le système et les clients ne recevront pas ce contenu.

Trace

Si vous cochez cette option et que vous recevez un contenu incluant les mots clés associés, le système enregistrera l'heure, l'adresse IP et le numéro de port du périphérique émetteur du contenu, l'adresse IP et le numéro de port du destinataire, ainsi que les mots clés trouvés.

Attention : vous pouvez activer l'option Rejeter, l'option Trace ou les deux à la fois suivant votre cas. Si aucune des deux n'est sélectionnée, la fonction Filtrage de mots clés est automatiquement désactivée.

Blocage d'URL

Entrez les URL que vous jugez indésirables et que vous souhaitez bloquer. Cliquez sur **Ajouter** pour que l'URL soit prise en compte. Pour supprimer une règle, cochez la case **Supprimer** correspondante.

IP autorisées

Les IP autorisées ont la priorité la plus haute. Cela signifie qu'en cas de conflit entre les règles de la fonction IP autorisées et celle de la fonction **Blocage d'URL** ou autre, les règles de la fonction IP autorisées ont la priorité. Entrez les plages d'adresses IP et de numéros de port dans les champs réservés à cet effet. Cliquez sur **Ajouter**. Pour supprimer une règle, cochez la case appropriée.

Ports filtrés

Les sites Web utilisent généralement le port 80. Certains en utilisent d'autres. Vous pouvez ajouter manuellement des numéros de port à la liste. Saisissez le numéro de port (80:888, par exemple) dans le champ approprié, puis cliquez sur **Ajouter**. Les ports entrés seront analysés et filtrés par mesure de sécurité. Si vous n'entrez aucune valeur, tous les ports seront filtrés. Pour désactiver une règle, cochez la case **Supprimer** correspondante. Cliquez sur **Tout effacer** pour effacer toutes les règles.

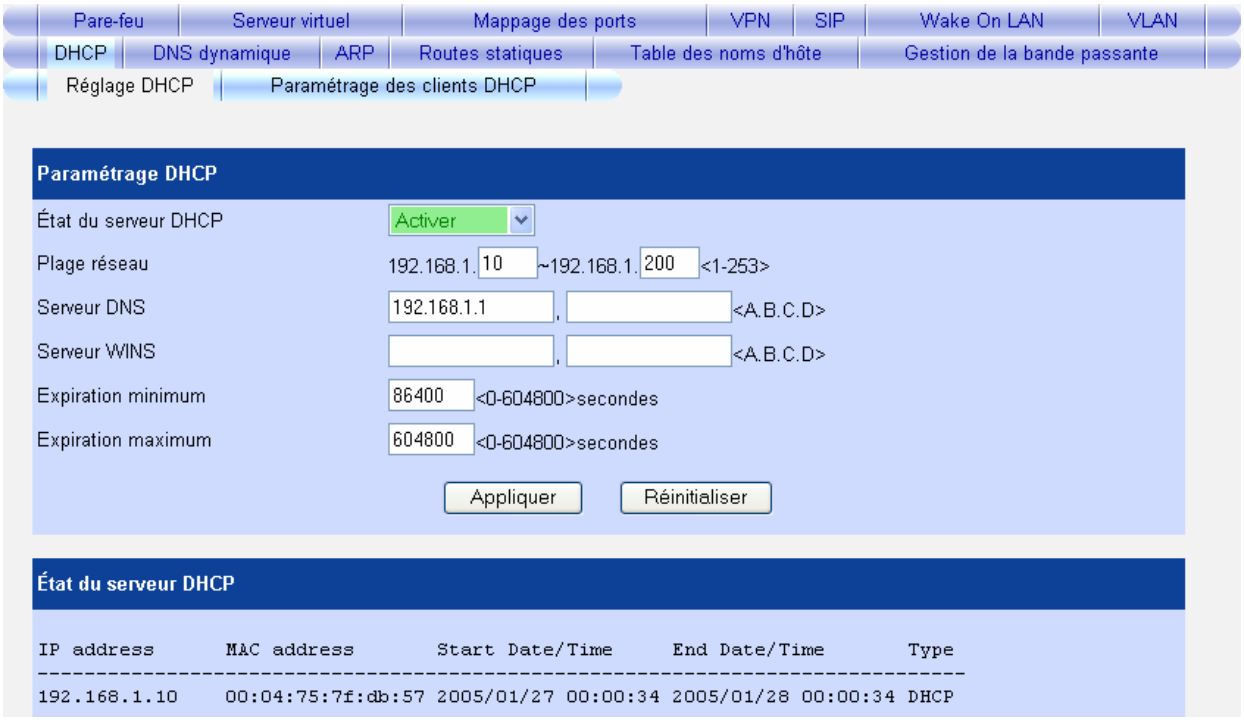
Attention : le port 80 figure par défaut dans la liste. Si vous effacez toutes les règles, tous les paquets seront filtrés.

Réglages avancés

DHCP

REGLAGE DHCP

Un serveur DHCP attribue automatiquement une adresse IP à chaque ordinateur du réseau. Sauf si vous en avez déjà un, il est fortement recommandé d'activer le serveur DHCP du système.



État du serveur DHCP

Sélectionnez **Activer** pour activer le serveur DHCP, **Désactiver** pour le désactiver ou **Redémarrer** pour le redémarrer.

Si l'état du serveur DHCP est défini sur **Désactiver**, cliquez sur le bouton **Appliquer** pour que les modifications soient prises en compte. Si l'état du serveur DHCP est défini sur **Activer**, cliquez sur le bouton **Réinitialiser** pour qu'elles le soient.

Plage réseau

Définissez la plage d'adresses IP que le serveur DHCP peut attribuer.

Serveur WINS

WINS est l'acronyme de Windows Internet Name Service (service WINS). C'est lui qui fournit au client DHCP le nom NetBIOS. Il met également en relation le nom de domaine avec l'adresse IP correspondante.

Expiration minimum

Il s'agit de la durée par défaut pendant laquelle un client DHCP peut conserver l'adresse IP si aucun délai d'expiration n'est spécifié.

Expiration maximum

Les clients DHCP ne peuvent demander qu'une durée de bail inférieure à cette valeur. Si la durée de bail demandée est supérieure à l'Expiration maximum, le système utilise par défaut cette valeur.

État du serveur DHCP

Cette section affiche les informations des clients DHCP, notamment l'adresse IP attribuée et la durée du bail.

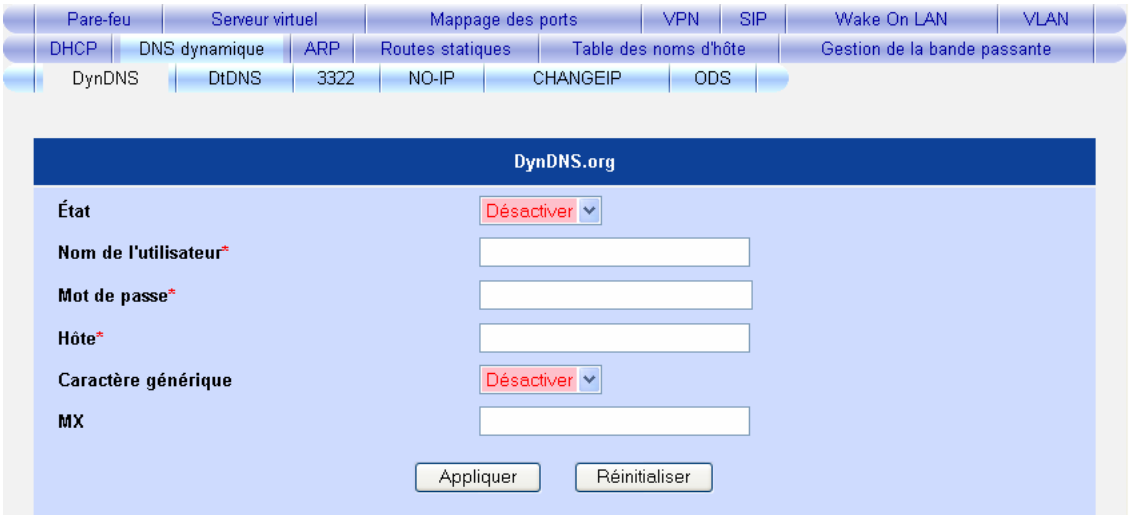
PARAMETRAGE DES CLIENTS DHCP

Les adresses IP peuvent être attribuées automatiquement, mais vous pouvez également les attribuer manuellement à certains périphériques. Pour ce faire, saisissez respectivement le nom du périphérique, son adresse IP et l'adresse MAC de sa carte réseau. Les trois premières colonnes doivent obligatoirement être renseignées. Les deux dernières peuvent être ignorées. Pour les serveurs nécessitant un fichier de démarrage placé sur un autre serveur, veillez à indiquer respectivement le fichier de démarrage en question et l'adresse IP du serveur TFTP (***T**rivial **F**ile **T**ransfer **P**rotocol*). Après avoir entré tous les paramètres, cliquez sur **Ajouter**. Pour supprimer une règle, cochez la case **Supprimer**, puis cliquez sur **Supprimer**. Pour annuler la suppression, cliquez sur **Réinitialiser**.

DNS dynamique

La fonction DNS (***D**omain **N**ame **S**ystem*) dynamique permet à l'utilisateur d'exporter un nom d'hôte vers Internet via un service de DNS dynamique. Tout utilisateur connecté à Internet peut ainsi accéder au routeur à l'aide d'un nom prédéfini enregistré chez ce fournisseur.

Au préalable, avant de procéder au paramétrage du DNS dynamique via l'interface du routeur, vous devez avoir ouvert un compte chez un des fournisseurs de noms de domaine dynamique actuellement supportés par le routeur. Ce compte une fois ouvert vous permettra de créer un lien dynamique entre le nom de domaine et l'adresse IP obtenue lors de chacune de vos connexions. La fonction DNS dynamique met automatiquement à jour l'adresse IP chez le fournisseur de service de DNS dynamique. Cela évite ainsi de fournir à chaque fois son adresse IP à un correspondant qui veut se connecter en ftp ou http par exemple sur votre serveur.



La série BeWAN Secure 50 prend en charge les services DynDNS, DtDNS, 3322, HN, NO-IP, CHANGEIP et ODS.

Après avoir créé un compte, renseignez les différents champs : le nom d'utilisateur et le mot de passe (fournis par le service sauf si vous avez modifié ce mot de passe) et le nom de l'hôte (nom choisi lors de la création de votre compte).

Sélectionnez **Activer** dans la liste déroulante **État**, puis cliquez sur **Appliquer** pour confirmer les paramètres.

Supposons que le nom de domaine soit runner.homelinux.net et que votre adresse e-mail soit theone@runner.homelinux.net. Si vous avez un serveur de messagerie et que vous avez déjà configuré un serveur virtuel (pour les e-mails) sous **Réglages avancés** > **Serveur virtuel**, votre serveur de messagerie peut recevoir/envoyer des e-mails si la fonction DNS dynamique est activée.

Supposons que vous n'ayez pas de serveur de messagerie et que vous utilisiez un serveur de messagerie (par exemple, mail.flying.net) basé sur Internet pour recevoir les messages envoyés à theone@runner.homelinux.net. Entrez dans ce cas mail.flying.net dans le champ **MX**. Les e-mails destinés à theone@runner.homelinux.net seront redirigés vers theone@mail.flying.net. L'avantage de cette fonction est que vous pouvez accéder à vos e-mails tant que le champ **MX** est correctement renseigné, même en cas de modification du serveur de messagerie.

Si la fonction **Caractère générique** est activée, tous les noms de domaine se terminant par runner.homelinux.net (par exemple, www.runner.homelinux.net ou vod.runner.homelinux.net) seront redirigés vers runner.homelinux.net. En d'autres termes, les noms de domaine se terminant par le caractère générique auront la même adresse IP.

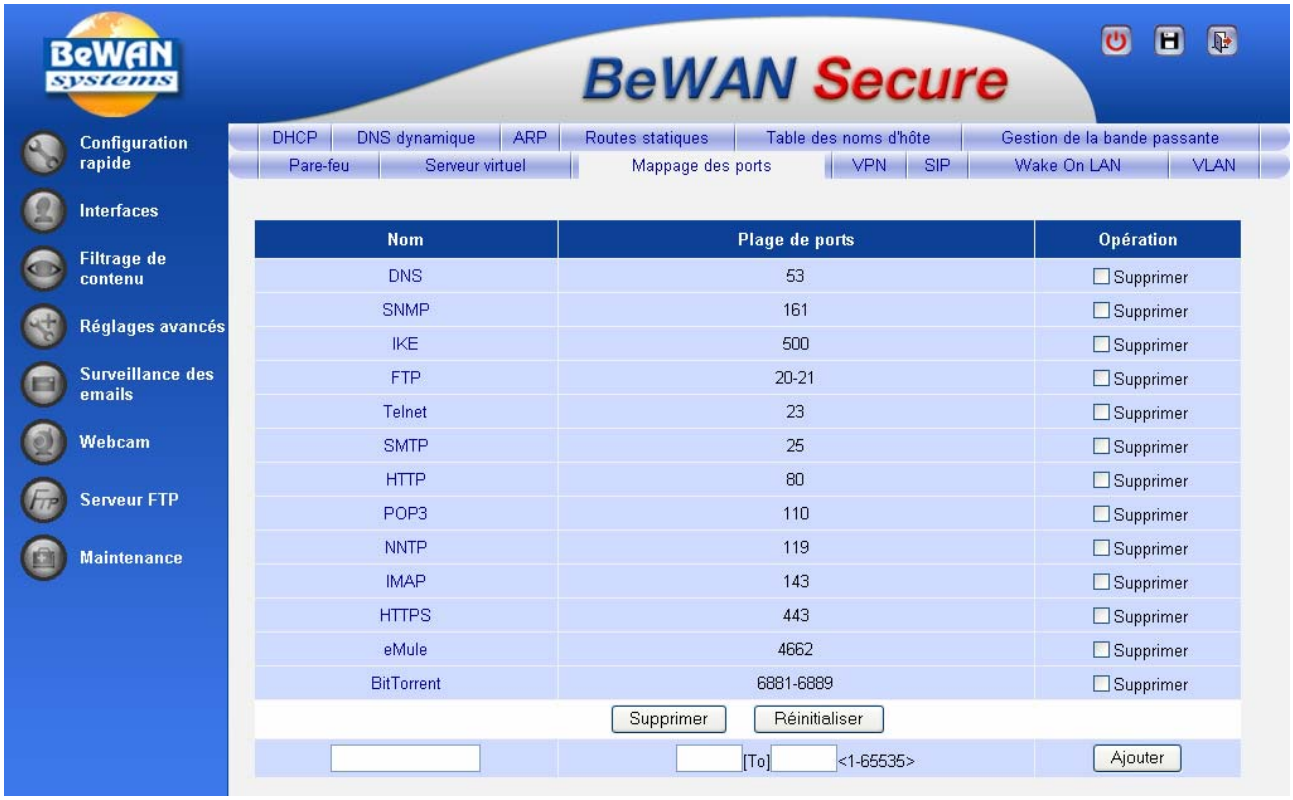
Mappage des ports

Si tous les programmes de serveur ne s'exécutent pas sur le même hôte, ou si vous ne souhaitez pas que les paquets (de service indisponible) soient redirigés vers le réseau local, vous pouvez spécifier des serveurs virtuels pour les différents types de services.

Supposons par exemple que l'ordinateur hôte ayant l'adresse IP 192.168.1.80 soit le serveur http, utilisant le protocole TCP avec le numéro de port 8000. Deux autres hôtes (192.168.1.11 et 192.168.1.12) exécutent FTP, utilisant le protocole TCP (UDP fermé) avec, respectivement, le numéro de port 21 et 2021.

Ajoutez le mappage de port à la liste. FTP est le service intégré par défaut s'exécutant avec le protocole TCP via le port 21.

La capture d'écran ci-dessous présente la liste des services par défaut du système.



Un mappage de port se compose d'un **Nom** et d'une **Plage de ports**. Par exemple, pour le mappage de port Internet, le nom peut être HTTP et le port utilisé est généralement le 80. Tous les mappages de port courants figurent déjà dans la liste. Pour ajouter un mappage de port, entrez respectivement le nom et la plage de ports, puis cliquez sur **Ajouter**.

Pour supprimer un mappage de port, cochez la case **Supprimer** correspondante et cliquez sur le bouton **Supprimer**. Le bouton **Réinitialiser** permet d'annuler une sélection.

Pare-feu

Consultez la section **Mappage des ports** avant de continuer.

REGLAGE

Le pare-feu est divisé en plusieurs sections :

Bloquer les Echo-Request du WAN

Si cette fonction est désactivée, le routeur envoie un paquet ICMP en réponse à l'envoi d'un paquet ICMP Echo-Request par les outils ping, traceroute ou autres. Il est recommandé d'activer cette option pour plus de sécurité.

Protection WAN

Lorsque cette option est activée, le routeur rejette les paquets provenant du réseau étendu ne correspondant pas à l'adresse IP spécifiée. Il est recommandé d'activer cette option lorsque vous activez la fonction NAT.

Pare-feu sur VPN

Permet d'appliquer les règles du pare-feu aux tunnels VPN.

REGLES

Les règles de pare-feu permettent de bloquer ou d'autoriser certains paquets. Par exemple, si vous avez un serveur SSH (Secure Shell) et que vous souhaitez que seuls les serveurs de votre entreprise puissent s'y connecter, vous devez mettre en œuvre des règles de pare-feu.

Attention : les règles de pare-feu sont mises en œuvre de haut en bas. Si une règle correspond, le système ne compare pas les suivantes. Si aucune règle ne correspond, le système autorise par défaut le paquet.

En l'absence de règles de pare-feu, le routeur autorise tous les paquets transmis du réseau local au réseau étendu. Pour les paquets transmis du réseau étendu au réseau local, les règles sont les suivantes :

Paquet W L'IP source est sur le réseau étendu et l'IP de destination est sur le réseau local.

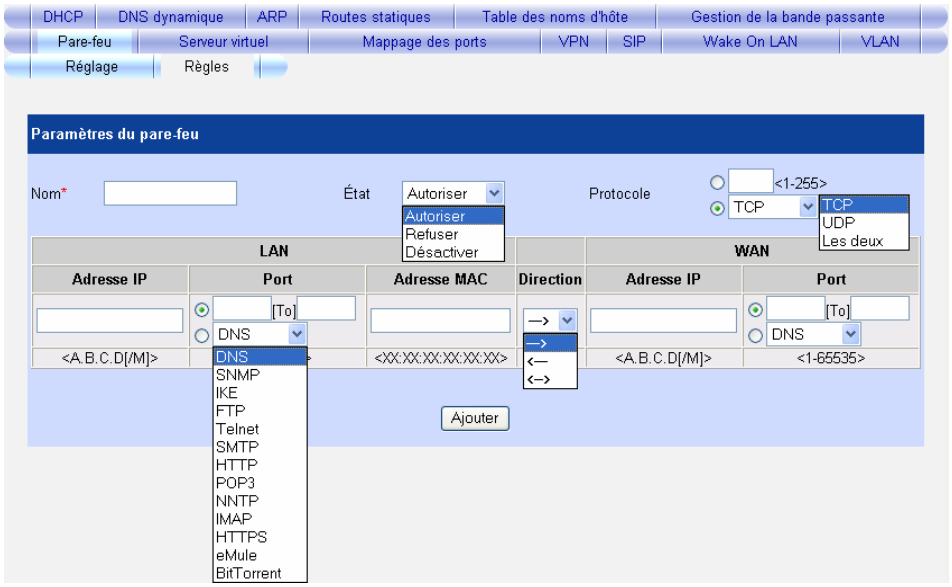
Paquet I L'IP source est sur le réseau étendu et l'IP de destination est celle de l'interface WAN du routeur.

Paquet N Paquets de réponse provenant du réseau étendu initiés par le réseau local.

	Protection WAN	NAT	Hôte DMZ	Serveur virtuel	Paquet autorisé
1	Non	Non			Paquet W
2	Non	Oui			Paquet W, Paquet N
3	Oui	Non			Non
4	Oui	Oui	Non	Non	Paquet N
5	Oui	Oui	Oui	Non	Paquet N Paquet I redirigé vers l'hôte
6	Oui	Oui	Non	Oui	Paquet N, paquet I correspondant redirigé vers le serveur virtuel
7	Oui	Oui	Oui	Oui	Paquet N Paquet I redirigé vers le serveur

Supposons que l'adresse IP du serveur soit 123.1.1.1. Pour poursuivre notre exemple, vous devez ajouter deux règles de pare-feu. La première doit autoriser les paquets SSH avec l'adresse IP 123.1.1.1 transmis du réseau étendu vers le réseau local. La seconde doit refuser les paquets SSH avec d'autres adresses IP transmis du réseau étendu au réseau local.

Cliquez tout d'abord sur **Règles**. La capture d'écran ci-dessous présente l'ajout de la première règle.



Nom

Nom de la règle de pare-feu. Vous pouvez saisir ce que vous voulez.

État

Autoriser, pour autoriser les paquets. **Refuser**, pour refuser les paquets. **Désactiver**, pour désactiver la règle. Les paquets ne sont pas filtrés.

Protocole

Vous pouvez entrer le numéro du protocole ou sélectionner **TCP**, **UDP** ou **Les deux**. Par exemple, le numéro de protocole de l'IPSec ESP est 50, et celui de l'IPSec AH est 51.

Direction

←, les paquets sont transmis du réseau étendu au réseau local.

→, les paquets sont transmis du réseau local au réseau étendu.

←→, les paquets proviennent soit du réseau local, soit du réseau étendu.

Adresse MAC

Il s'agit de l'adresse MAC source des paquets. Pour les paquets entrants, l'adresse MAC source sera celle de l'hôte WAN ; pour les paquets sortants, ce sera celle de l'hôte LAN.

Adresse IP

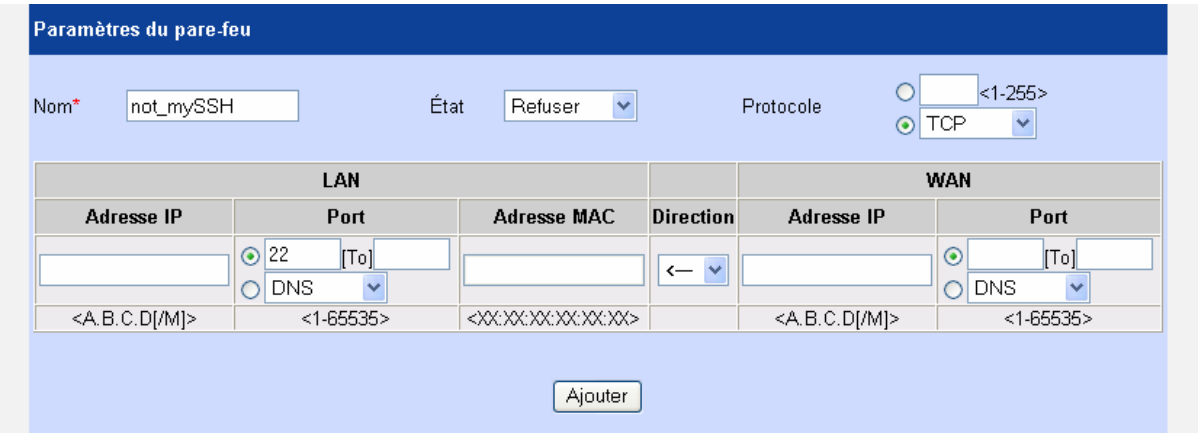
Il s'agit de l'adresse IP source/de destination des paquets. L'adresse IP peut comporter des sous-réseaux, c'est-à-dire 123.1.1.0/24.

Port

Mappage de port. Vous pouvez activer un mappage de port précis ou entrer un port manuellement. Si vous souhaitez que le type de service ne soit pas pris en compte, ne renseignez pas ce champ.

Lorsque vous cliquez sur **Ajouter**, l'écran suivant devrait apparaître :

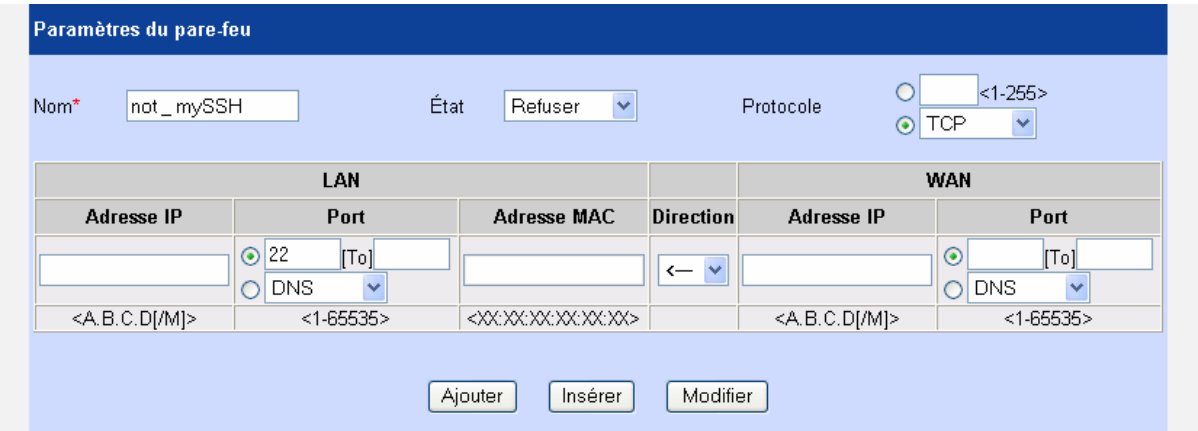
Cliquez sur **Ajouter** pour ajouter la seconde règle de pare-feu.



Cliquez sur **Ajouter**. L'écran suivant devrait apparaître :

Pour modifier l'ordre des règles du pare-feu, utilisez les flèches de la colonne **Déplacer**. La dernière règle créée est toujours placée au bas de la liste. Pour supprimer une règle, cochez la case de la colonne **Supprimer** et cliquez sur le bouton **Supprimer**.

Pour modifier une règle, cliquez sur son nom au début de la ligne. La page suivante apparaît :

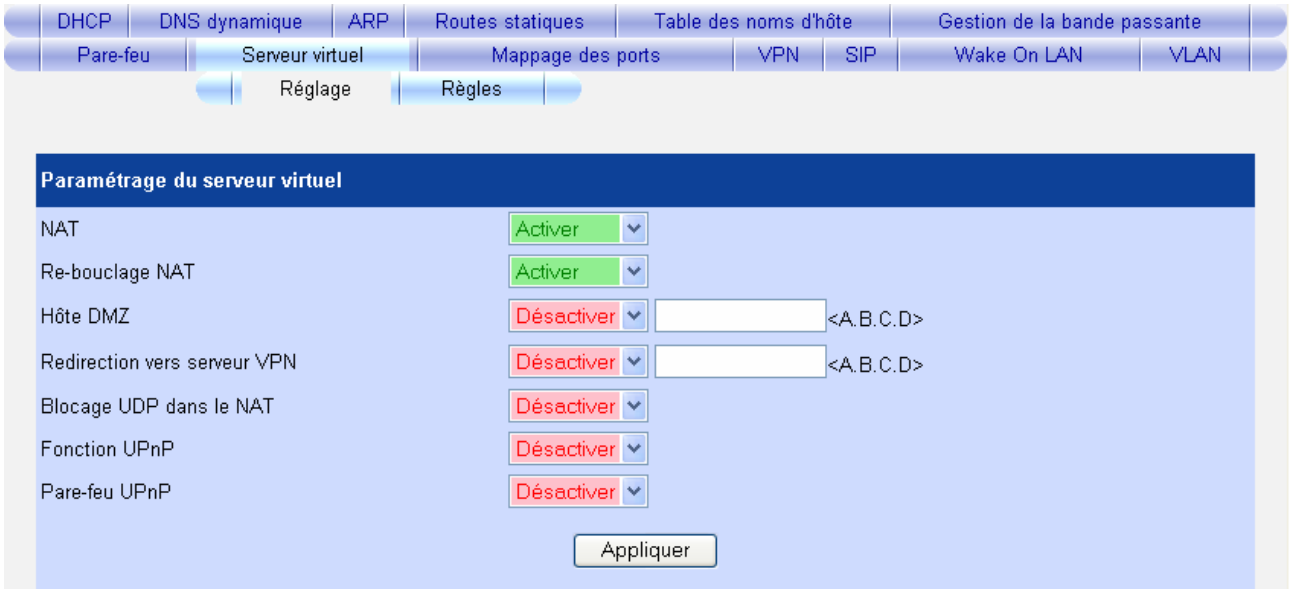


Cette page est similaire à celle permettant de créer une règle, mais elle comporte les boutons **Insérer** et **Modifier**. Le bouton **Modifier** permet d'activer le nouveau paramétrage, les modifications ne sont pas enregistrées dans la mémoire flash. Le bouton **Insérer** permet d'insérer une règle dans la ligne en cours.

Serveur virtuel

Si vous avez un serveur de messagerie, HTTP ou de fichiers (dans votre réseau local) et que vous souhaitez y accéder depuis le réseau étendu, vous devez configurer les serveurs virtuels nécessaires. Pour les applications peer-to-peer, un serveur virtuel doit également être configuré.

REGLAGE



La capture d'écran ci-dessus présente les paramètres du serveur virtuel.

NAT

L'hôte doit avoir une adresse IP publique pour pouvoir communiquer avec les autres sur Internet. En raison du manque d'adresses IP, le FAI fournit une adresse IP dynamique et non statique. Cela signifie que l'adresse IP est différente à chaque connexion. Ceux qui ont besoin d'une adresse IP statique doivent payer plus cher. La plupart des particuliers ou des réseaux SOHO utilisent l'une ou l'autre.

Une adresse IP publique étant requise pour pouvoir communiquer avec les autres sur Internet, une fonction NAT est nécessaire si plusieurs serveurs souhaitent se connecter à Internet. La fonction NAT (***N**etwork **A**ddress **T**ranslation*) effectue la traduction des adresses entre le réseau local et le réseau étendu.

Veuillez activer cette fonction dans les situations décrites ci-dessus.

Re-bouclage NAT

Cette fonction permet de rediriger les paquets vers le serveur virtuel lorsque la demande est initiée depuis le réseau local. Après avoir configuré l'hôte DMZ ou le serveur virtuel, vous pouvez configurer le nom de domaine correspondant (en cas d'adresse IP dynamique, utilisez la fonction DNS dynamique intégrée) pour en faciliter l'accès. Vous pourrez ainsi accéder facilement au service que vous configurez depuis Internet via ce nom de domaine. Pour pouvoir accéder à ce service depuis le réseau local avec le même nom de domaine, activez la fonction **Re-bouclage NAT**. Ainsi, que vous soyez sur Internet ou sur le réseau local, vous pouvez accéder au service configuré en utilisant le même nom de domaine.

Hôte DMZ

Si des serveurs de votre réseau local sont configurés pour fournir des services aux autres, vous devez configurer un hôte DMZ ou des serveurs virtuels.

Si tous les serveurs sont sur le même ordinateur hôte dans le réseau local, vous pouvez choisir de configurer un hôte DMZ.

Une fois ce dernier configuré, toutes les requêtes entrantes provenant du réseau étendu sont redirigées vers lui. Ceci a l'avantage de faciliter l'installation. L'inconvénient est que tous les programmes de serveur doivent se trouver sur le même ordinateur hôte et que tous les paquets sont dirigés vers l'hôte quelle que soit la disponibilité du service.

Pour configurer un hôte DMZ, saisissez l'adresse IP qui lui a été attribuée dans votre réseau intranet. Sélectionnez **Activer** dans la liste déroulante **État**, puis cliquez sur **Appliquer**. Pour désactiver l'hôte DMZ, sélectionnez **Désactiver** dans la liste déroulante **État**, puis cliquez sur **Appliquer**.

Redirection vers serveur VPN

Si vous avez créé un serveur PPTP au sein de votre réseau local et que vous souhaitez établir une connexion VPN à ce serveur depuis Internet, il vous suffit d'indiquer son adresse IP, de sélectionner **Activer** et de cliquer sur **Appliquer**.

Blocage UDP dans le NAT

Cette fonction est désactivée par défaut. Cela signifie que le système ne bloque pas les paquets UDP.

Fonction UPnP

L'UPnP (***U**niversal **P**lug and **P**lay*) est une norme utilisant Internet et les protocoles Web pour permettre aux PC, périphériques, appareils intelligents et autres périphériques sans fil de se reconnaître automatiquement lorsqu'ils sont connectés à un réseau. Par exemple, si vous avez un ordinateur et une imprimante connectés au réseau et que vous devez imprimer un document, vous pouvez cliquer sur un bouton de l'ordinateur pour qu'il envoie une requête « Discover » afin de déterminer si une imprimante est connectée au réseau. L'imprimante s'identifie et indique son emplacement en envoyant une URL.

Attention : l'UPnP a un impact important sur la sécurité. Les routeurs/passerelles dont la fonction UPnP est activée peuvent ouvrir n'importe quel port du réseau local. Ceci représente une faille importante pour les virus et les chevaux de Troie.

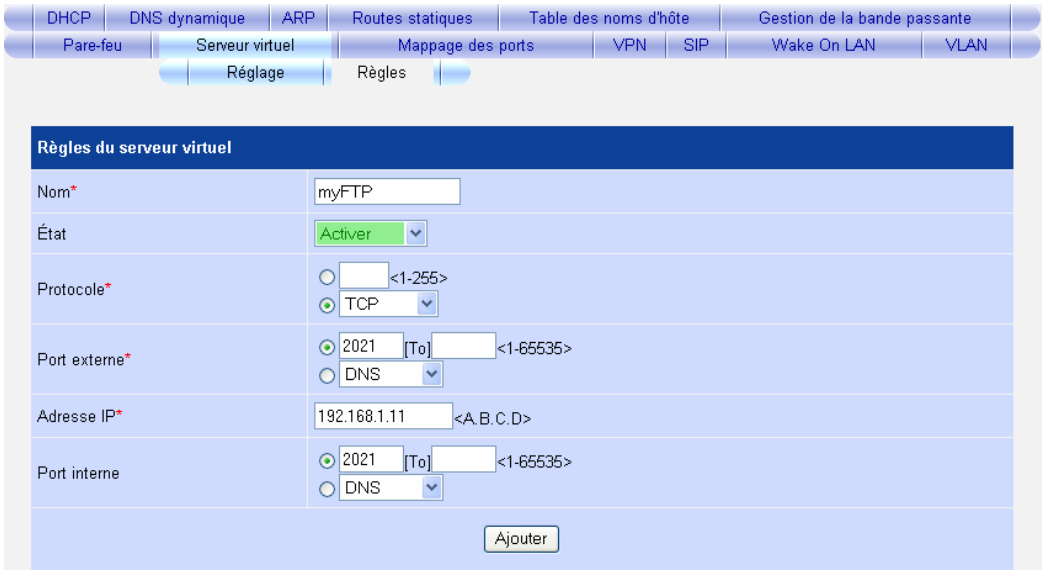
Sélectionnez **Activer** pour activer la fonction UPnP. Une fois activée, elle fournit la fonctionnalité DNAT (***D**estination **N**etwork **A**ddress **T**ranslation*) UPnP. Si l'application ou le jeu en ligne que vous utilisez requiert la prise en charge de l'UPnP, activez cette option.

Pare-feu UPnP

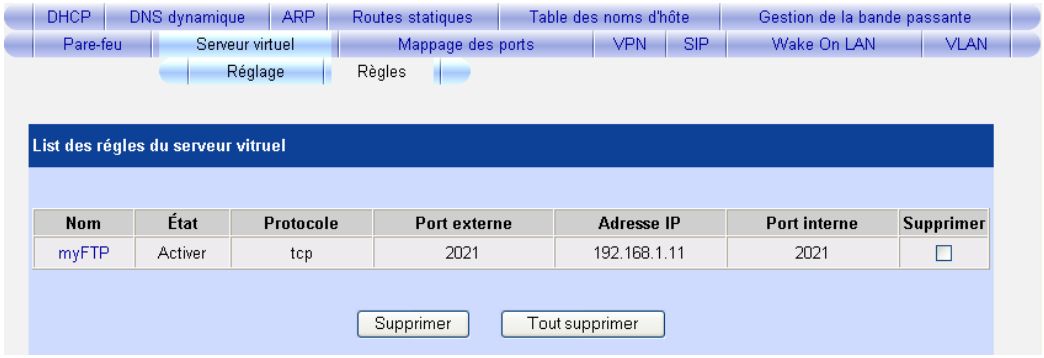
Si vous avez mis en œuvre des règles de pare-feu empêchant certains hôtes/services de se connecter à Internet, activez cette option pour qu'ils puissent communiquer avec le réseau étendu (WAN).

REGLES

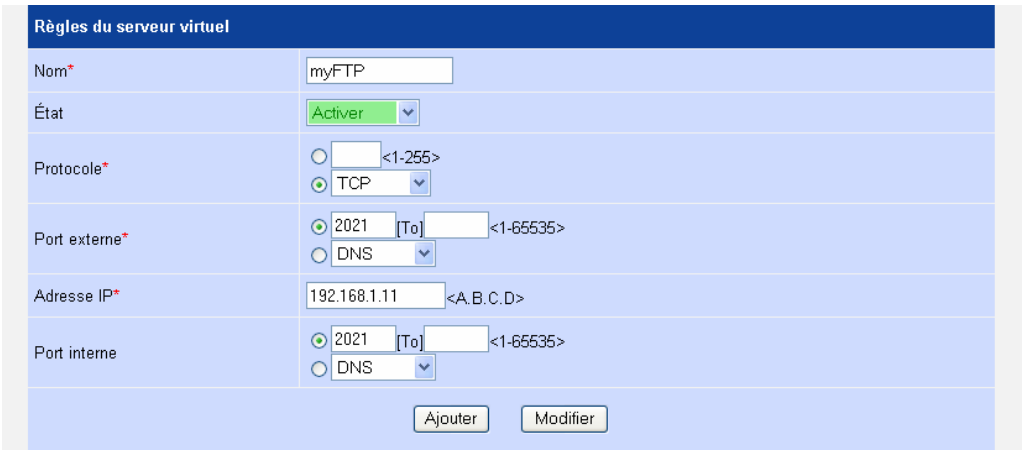
Sélectionnez **Réglages avancés** dans le menu principal, puis cliquez sur **Serveur virtuel**. Cliquez sur **Règles** pour ouvrir la page de configuration. Renseignez les champs puis cliquez sur **Ajouter**.



La page ci-dessous apparaît. Répétez la procédure si vous souhaitez ajouter d'autres serveurs virtuels.

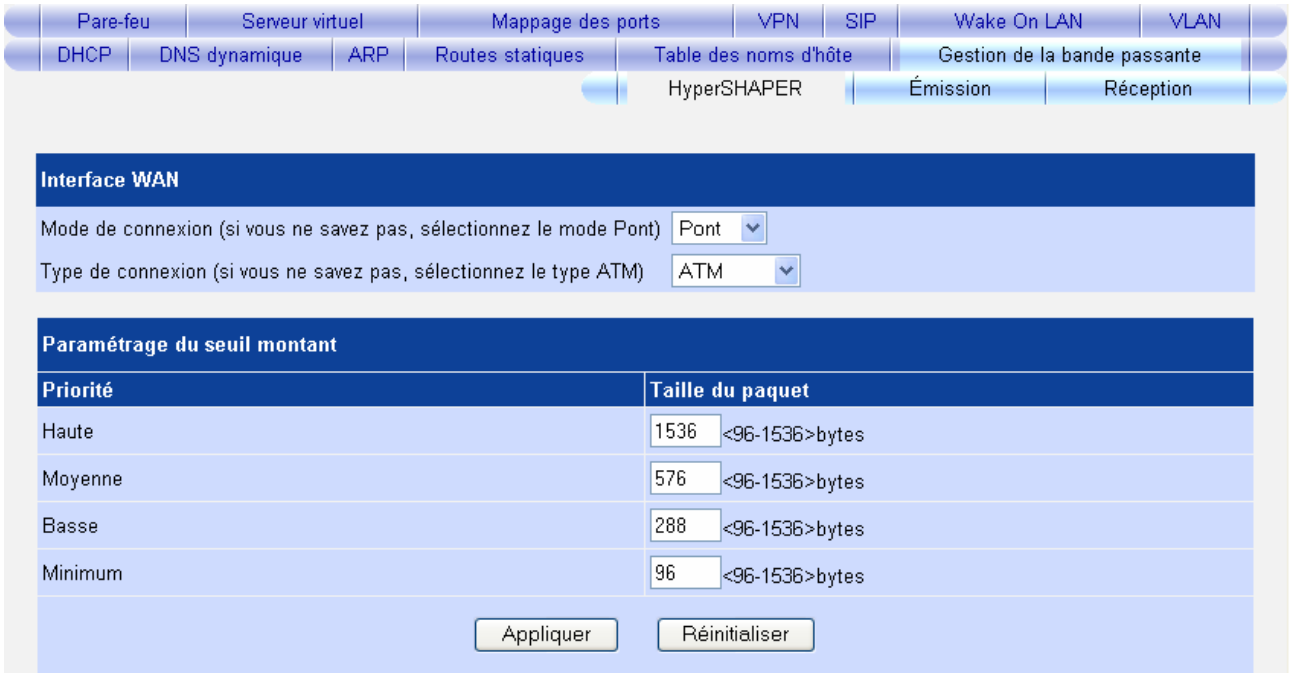


Pour modifier, activer/désactiver ou supprimer un serveur virtuel, cliquez sur son nom.



Cliquez sur **Modifier** pour que les modifications soient prises en compte. Les nouveaux paramètres ne sont pas sauvegardés dans la mémoire flash.

Gestion de la bande passante

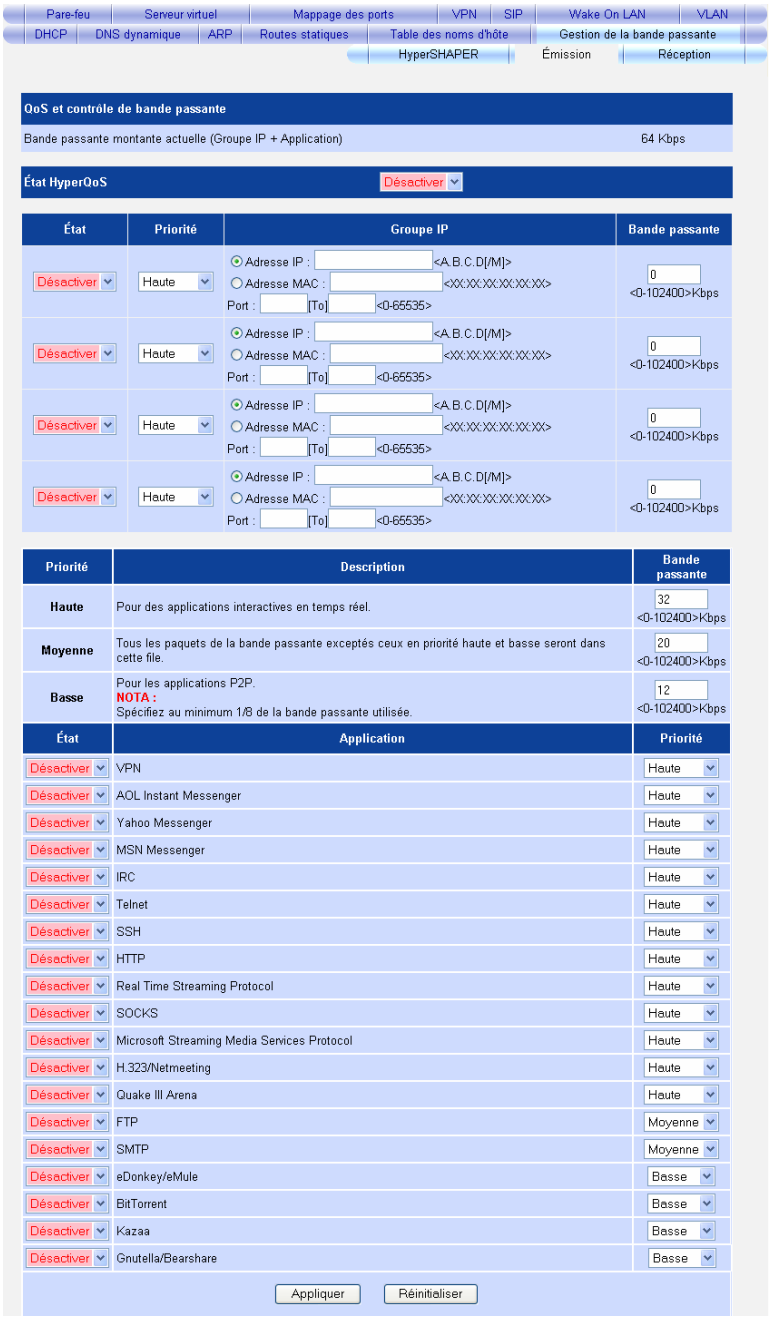


HYPERSHAPER

HyperQoS et HyperShaper sont implémentées pour améliorer votre expérience du peer-to-peer (P2P) et l'utilisation de l'audio et de la vidéo en temps réel sur Internet. Grâce à la technologie HyperSHAPER intégrée, le temps de réponse des applications réseau est considérablement amélioré.

HYPERQOS POUR L'EMISSION ET LA RECEPTION

Parallèlement à la fonction QoS (***Quality of Service***) standard, la fonction HyperQoS permet de surveiller l'état de la connexion et d'utiliser au maximum la bande passante en fonction du type de support de transmission. La gestion de la bande passante est composée de deux sections : **Émission** et **Réception**.



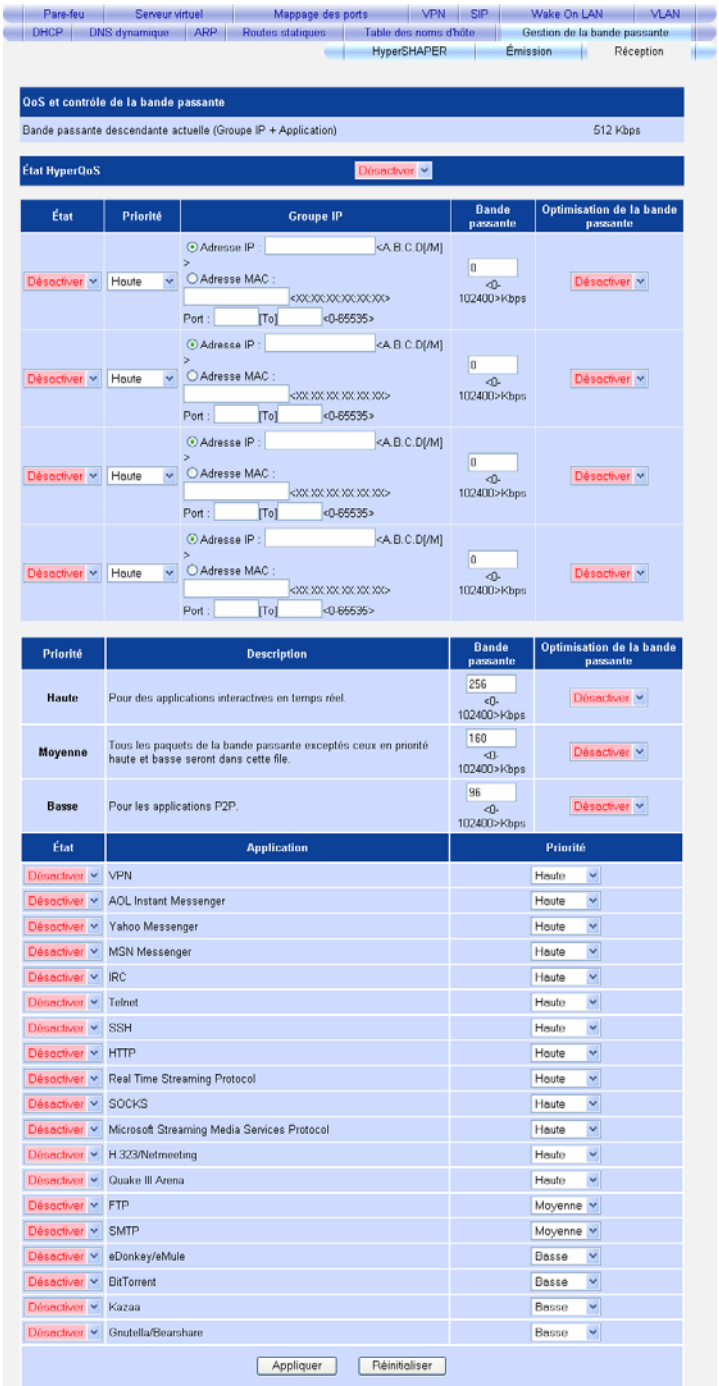
La capture d'écran ci-dessus présente l'onglet **Gestion de la bande passante**. La configuration consiste essentiellement à effectuer le paramétrage des seuils HyperSHAPER et de la fonction HyperQoS.

Sous HyperSHAPER, les tailles des paquets peuvent être définies pour chaque niveau de priorité. Les paquets seront fragmentés selon la valeur du seuil configurée pour chacun de ces niveaux. La taille des paquets est généralement plus importante pour le trafic prioritaire.

La fonction HyperQoS fonctionne conjointement avec la fonction HyperSHAPER. Les utilisateurs peuvent également spécifier une plage d'adresses IP et définir son niveau de priorité. Le trafic provenant d'une plage d'adresses IP donnée peut, par exemple, avoir la priorité la plus élevée et disposer d'une quantité définie de bande passante. Les utilisateurs peuvent activer ou désactiver certains états au début de chaque ligne. Dans la zone Description, indiquez la quantité de bande passante attribuée à chaque niveau de priorité. La quantité totale de bande passante attribuée ne doit pas excéder la bande passante montante disponible.

Une liste d'applications permet également de définir le niveau de priorité de chacune d'elles et de les activer/désactiver. Le niveau de priorité que vous définissez dans cette liste suit les critères de priorité définis précédemment pour les fonctions HyperQoS et HyperSHAPER. Cliquez sur le bouton **Appliquer** pour que les modifications soient prises en compte.

La page de gestion de la bande passante descendante s'affiche ensuite. Elle est identique à la page de gestion de la bande passante montante, seul le sens du trafic est différent.



Chaque fois que le système tente d'envoyer un paquet, il sélectionne le paquet que la file d'attente de chaque configuration de bande passante veut envoyer en fonction du niveau de priorité. Le cas échant, le reste de la bande passante peut être prêté aux programmes qui en ont besoin en fonction de leur niveau de priorité (en commençant par les programmes prioritaires). Ainsi, la bande passante est non seulement préservée, mais également utilisée à son maximum.

Lors de la sélection des files d'attente, le système vérifie si l'adresse IP source du paquet correspond à l'un des quatre groupes IP. Le cas échéant, le paquet est placé dans la file d'attente du groupe IP correspondant. Si l'adresse IP source ne correspond à aucun des quatre groupes IP, le système contrôle le comportement de connexion et utilise la technologie de reconnaissance des empreintes de données pour déterminer l'application émettrice du paquet et placer ce dernier dans la file d'attente de l'application correspondante. **Vous pouvez utiliser une seule de ces deux approches de contrôle de la bande passante ou les combiner selon vos besoins : contrôle de la bande passante par hôte/sous-réseau et par type d'application.**

Durant l'envoi, le système fragmente les paquets en fonction de leur niveau de priorité. Ainsi, lors de l'envoi de paquets avec une priorité basse, le temps d'attente pour les paquets prioritaires est réduit, ce qui a pour effet d'accroître la vitesse de réponse des applications réseau en temps réel.

La fonction de gestion de la bande passante est puissante mais sa configuration est assez simple. **Veillez à utiliser des multiples de 48 pour le paramétrage des seuils HyperSHAPER pour une meilleure efficacité.** Plus le seuil HyperSHAPER d'un niveau de priorité est bas, plus le temps nécessaire à l'envoi d'un paquet de ce niveau de priorité est court ; même si l'efficacité de l'envoi s'en trouve légèrement affectée, la vitesse de transmission globale peut être augmentée. Si le seuil HyperSHAPER d'un niveau de priorité est défini sur la valeur maximale (1536), les paquets de ce niveau de priorité ne seront pas fragmentés par le système. Après avoir défini le seuil HyperSHAPER de chaque niveau de priorité, cliquez sur le bouton **Appliquer** correspondant pour activer le paramétrage.

*Remarque : la fonction HyperQoS doit être **Activée** pour pouvoir activer la fonction HyperSHAPER.*

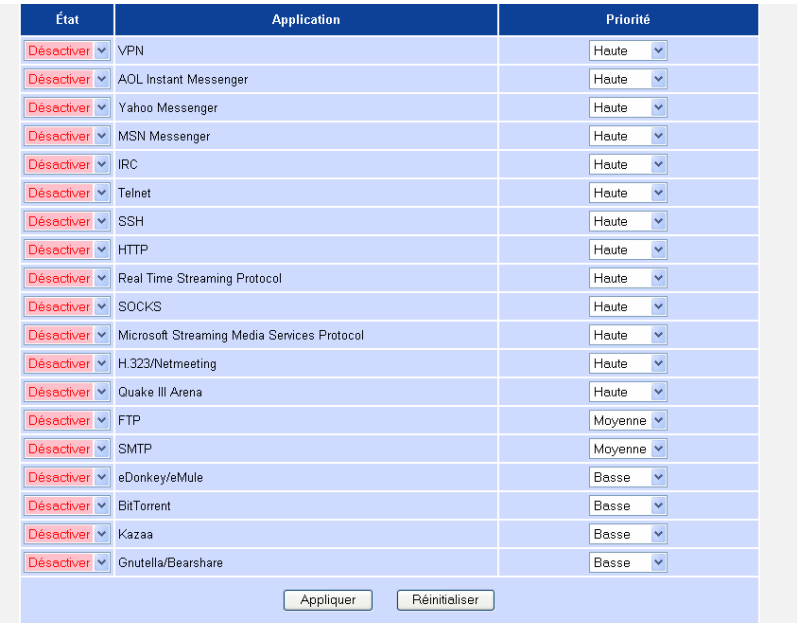
Comme pour la fonction HyperQoS, veuillez suivre les instructions ci-dessous :

- Déterminez quels groupes IP et quelles applications vous souhaitez configurer, ainsi que les quantités de bande passante à allouer et les niveaux de priorité à attribuer.
- Saisissez l'adresse IP ou le sous-réseau.
- Saisissez la quantité de bande passante allouée.
- Définissez le niveau de priorité.
- Activez la file d'attente IP ou l'application.
- Activez l'état HyperQoS.
- Vérifiez que la bande passante montante affichée correspond à celle de votre connexion Internet.
- Cliquez sur **Appliquer** pour que les modifications soient prises en compte.

Comme sur la capture d'écran précédente, les quatre files d'attente des hôtes/sous-réseaux sont désactivées, celles des priorités haute, moyenne et basse ont respectivement une bande passante montante de 32, 20 et 12 Kbps (k/bits par seconde), et le niveau de priorité de chaque application est défini.

Le trafic dont la priorité n'est pas explicitement définie recevant la priorité moyenne, il n'est pas nécessaire de définir la priorité des applications FTP (***F**ile **T**ransfer **P**rotocol*) et SMTP (***S**imple **M**ail **T**ransfer **P**rotocol*) sur **Moyenne** dans l'exemple ci-dessus.

Pour transférer de l'audio et de la vidéo en temps réel sur le réseau ou participer à un jeu en ligne, il est recommandé de ne pas définir la priorité des autres types de trafic sur **Haute**. Ceci est illustré dans la capture d'écran suivante :



État	Application	Priorité
Désactiver	VPN	Haute
Désactiver	AOL Instant Messenger	Haute
Désactiver	Yahoo Messenger	Haute
Désactiver	MSN Messenger	Haute
Désactiver	IRC	Haute
Désactiver	Telnet	Haute
Désactiver	SSH	Haute
Désactiver	HTTP	Haute
Désactiver	Real Time Streaming Protocol	Haute
Désactiver	SOCKS	Haute
Désactiver	Microsoft Streaming Media Services Protocol	Haute
Désactiver	H.323/Netmeeting	Haute
Désactiver	Quake III Arena	Haute
Désactiver	FTP	Moyenne
Désactiver	SMTP	Moyenne
Désactiver	eDonkey/eMule	Basse
Désactiver	BitTorrent	Basse
Désactiver	Kazaa	Basse
Désactiver	Gnutella/Bearshare	Basse

Appliquer Réinitialiser

Si le type de transfert audio et vidéo en temps réel sur le réseau ou le jeu en ligne que vous souhaitez utiliser ne figure pas dans la liste des applications intégrée, vous pouvez utiliser les files d'attente des hôtes/sous-réseaux pour configurer le contrôle de la bande passante et du trafic montant.

QoS et contrôle de la bande passante

Bande passante descendante actuelle (Groupe IP + Application) 512 Kbps

État HyperQoS Activer

État	Priorité	Groupe IP	Bande passante	Optimisation de la bande passante
Désactiver	Haute	Adresse IP : <A.B.C.D[/M]> Adresse MAC : <XX:XX:XX:XX:XX:XX> Port : [To] <0-65535>	0 <0-102400>Kbps	Désactiver
Désactiver	Haute	Adresse IP : <A.B.C.D[/M]> Adresse MAC : <XX:XX:XX:XX:XX:XX> Port : [To] <0-65535>	0 <0-102400>Kbps	Désactiver
Désactiver	Haute	Adresse IP : <A.B.C.D[/M]> Adresse MAC : <XX:XX:XX:XX:XX:XX> Port : [To] <0-65535>	0 <0-102400>Kbps	Désactiver
Désactiver	Haute	Adresse IP : <A.B.C.D[/M]> Adresse MAC : <XX:XX:XX:XX:XX:XX> Port : [To] <0-65535>	0 <0-102400>Kbps	Désactiver

Priorité	Description	Bande passante	Optimisation de la bande passante
Haute	Pour des applications interactives en temps réel.	256 <0-102400>Kbps	Désactiver
Moyenne	Tous les paquets de la bande passante exceptés ceux en priorité haute et basse seront dans cette file.	160 <0-102400>Kbps	Désactiver
Basse	Pour les applications P2P.	96 <0-102400>Kbps	Désactiver

VPN

Un réseau privé virtuel permet d'utiliser une infrastructure de télécommunication publique, telle qu'Internet, pour fournir à des filiales ou à des utilisateurs individuels un accès sécurisé au réseau de leur organisation.

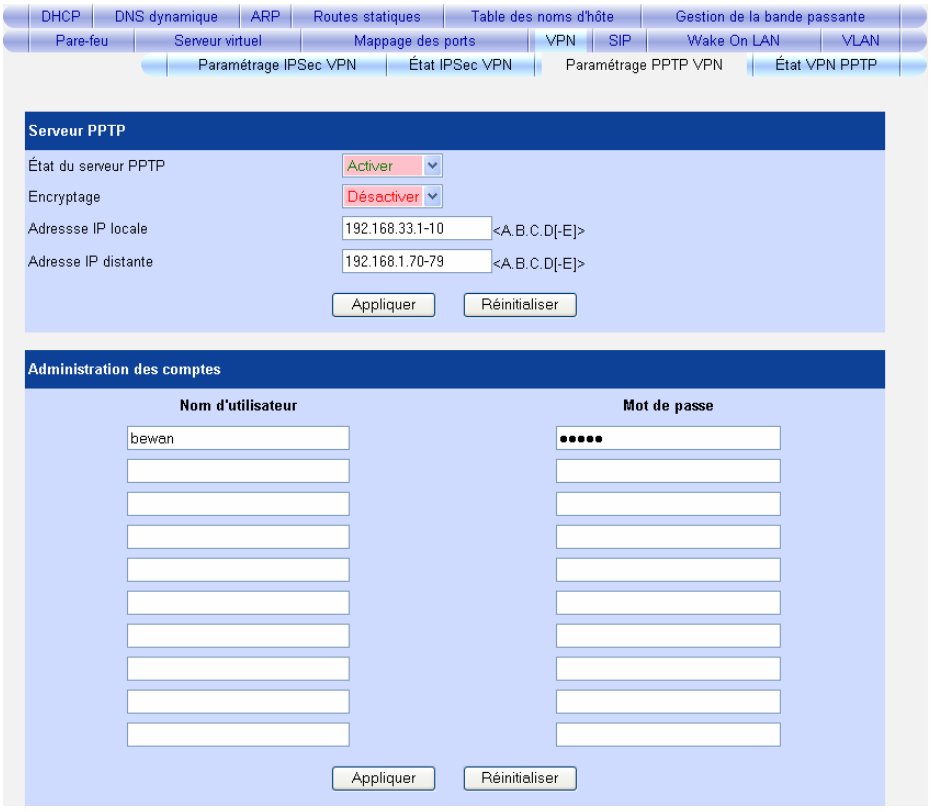
Un réseau VPN se base sur une infrastructure publique partagée tout en préservant la confidentialité à l'aide de procédures de sécurité et de protocoles de tunnellisation. Les données peuvent en outre être cryptées et faire appel à un algorithme d'authentification pour une plus grande confidentialité.

Le routeur prend en charge deux protocoles pour les réseaux VPN : le PPTP (***P**oint-to-**P**oint **T**unneling **P**rotocol*) et l'IPSec (***IP Sec**urity Protocol*). Le protocole PPTP offre la tunnellisation, tandis que le protocole IPSec offre la tunnellisation, l'authentification et le cryptage.

PARAMETRAGE PPTP VPN

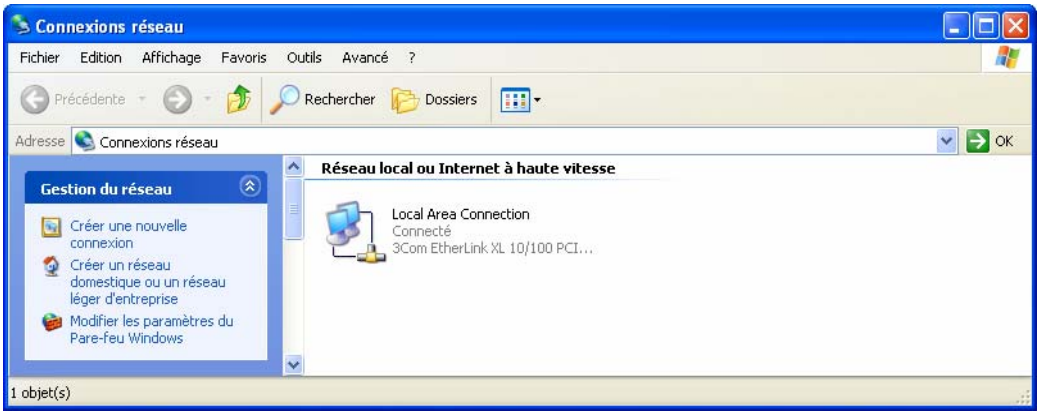
Le routeur prend en charge le protocole de tunnellisation PPTP. Les utilisateurs peuvent se connecter au réseau de leur entreprise via PPTP. Les BeWAN Secure série 50 prennent en charge jusqu'à 10 connexions PPTP. Pour configurer un serveur PPTP, cliquez sur **Paramétrage PPTP VPN**. Pour vérifier l'état du serveur PPTP, cliquez sur **État VPN PPTP**.

La page de paramétrage du serveur PPTP est divisée en deux parties : **Serveur PPTP** et **Administration des comptes**. Supposons que l'adresse IP de l'interface LAN soit toujours celle par défaut, à savoir 192.168.1.1/24, que celle de l'interface WAN soit 192.168.2.1/24, que celle que nous souhaitons attribuer au client PPTP (**Adresse IP distante**) soit comprise entre 192.168.1.70 et 192.168.1.79, que l'**Adresse IP locale** soit comprise entre 192.168.33.1 et 192.168.33.10 et que nous créions le compte bewan (mot de passe : bewan), comme représenté sur l'illustration ci-dessous. Pour activer le serveur PPTP, activez la fonction **État du serveur PPTP**. Le routeur prend en charge l'algorithme de cryptage MPPE (***M**icrosoft **P**oint-to-**P**oint **E**ncryption*). Pour activer le cryptage des données du tunnel PPTP, activez la fonction **Encryptage**.

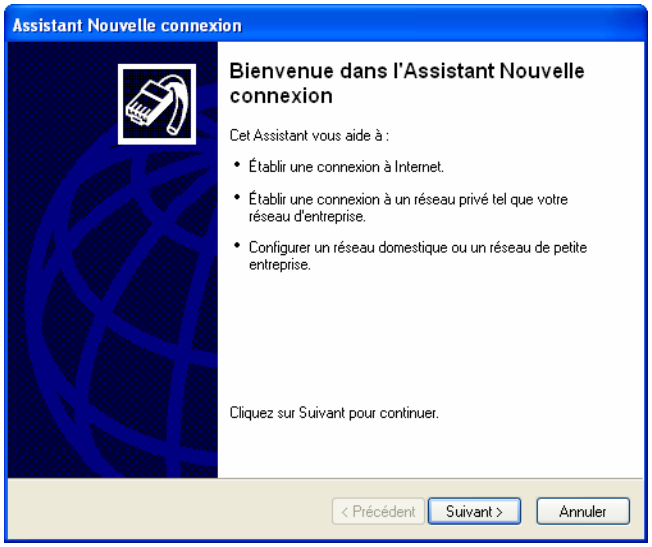


Après avoir effectué la configuration de base du serveur PPTP, cliquez sur le bouton **Appliquer** pour qu'elle soit prise en compte. Lorsque vous créez un compte, vous devez également cliquer sur le bouton **Appliquer** de la section **Administration des comptes** pour qu'il soit pris en compte.

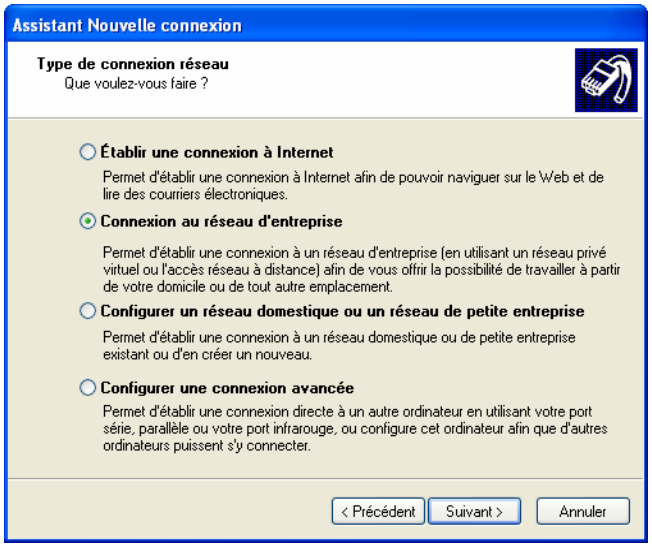
Pour la configuration du client PPTP, prenons l'exemple de Windows XP. Ouvrez la fenêtre **Connexions réseau**, puis cliquez sur **Créer une nouvelle connexion**.



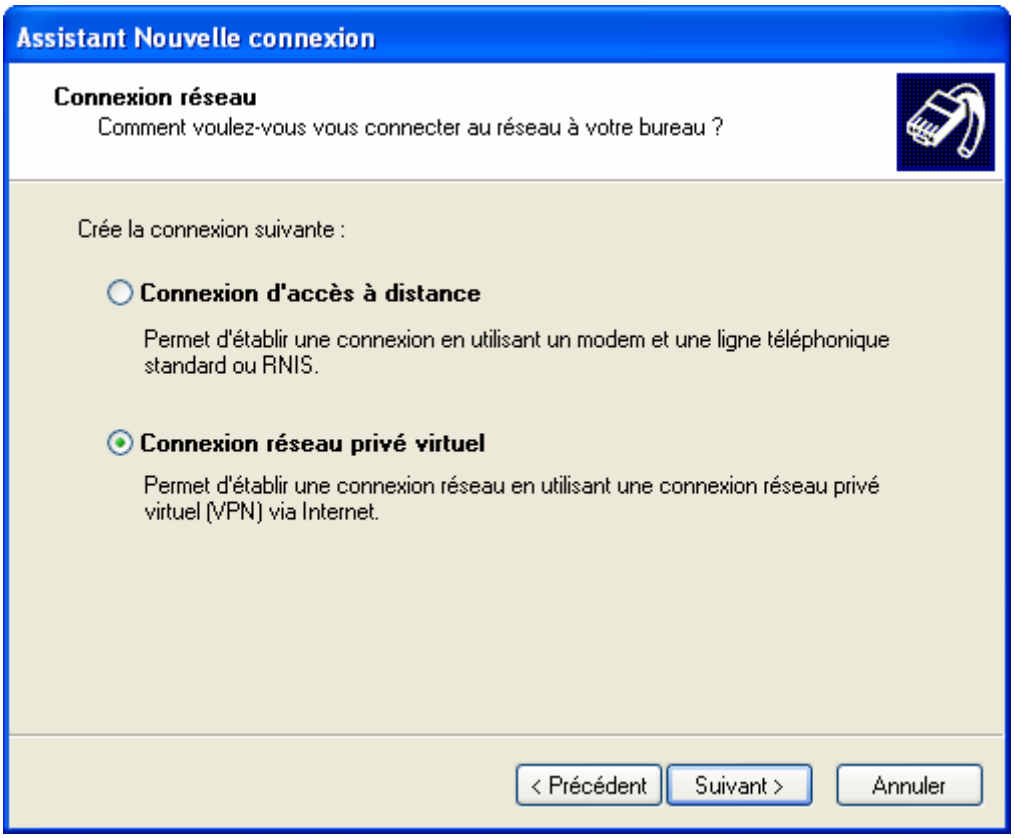
Cliquez sur **Suivant**.


Assistant Nouvelle connexion
Bienvenue dans l'Assistant Nouvelle connexion
Cet Assistant vous aide à :
• Établir une connexion à Internet.
• Établir une connexion à un réseau privé tel que votre réseau d'entreprise.
• Configurer un réseau domestique ou un réseau de petite entreprise.
Cliquez sur Suivant pour continuer.
< Précédent
Suivant >
Annuler

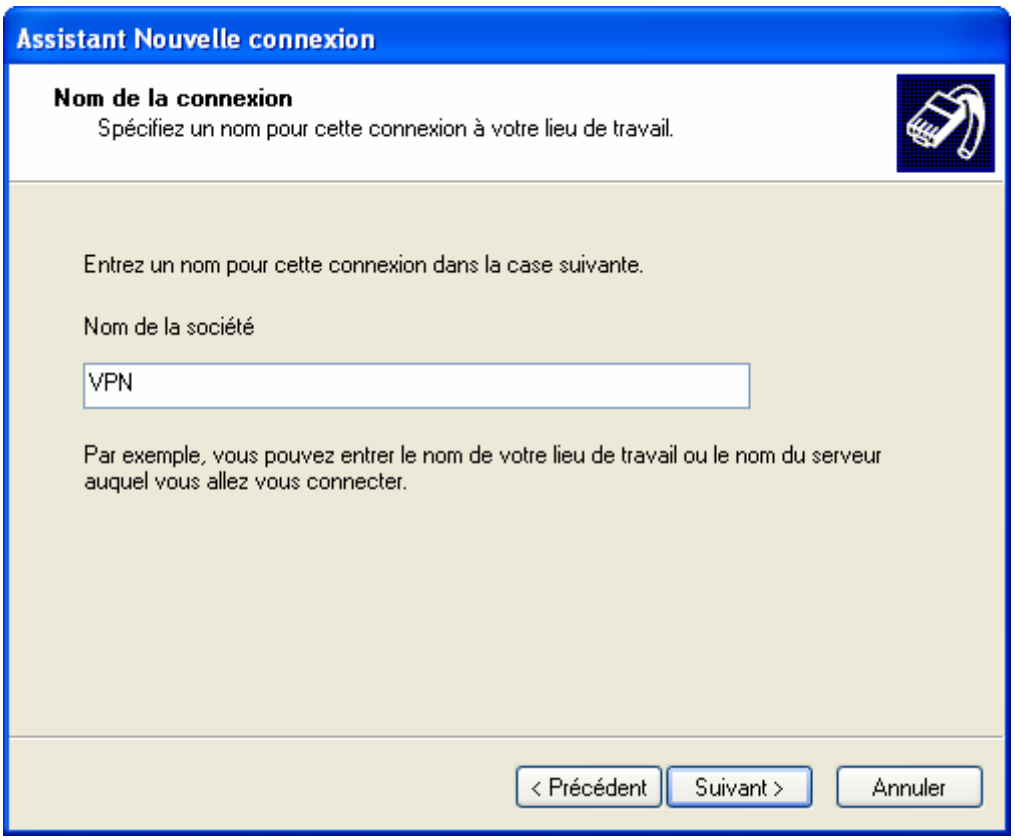
Sélectionnez **Connexion au réseau d'entreprise**. Cliquez sur **Suivant**.


Assistant Nouvelle connexion
Type de connexion réseau
Que voulez-vous faire ?
Établir une connexion à Internet
Permet d'établir une connexion à Internet afin de pouvoir naviguer sur le Web et de lire des courriers électroniques.
Connexion au réseau d'entreprise
Permet d'établir une connexion à un réseau d'entreprise (en utilisant un réseau privé virtuel ou l'accès réseau à distance) afin de vous offrir la possibilité de travailler à partir de votre domicile ou de tout autre emplacement.
Configurer un réseau domestique ou un réseau de petite entreprise
Permet d'établir une connexion à un réseau domestique ou de petite entreprise existant ou d'en créer un nouveau.
Configurer une connexion avancée
Permet d'établir une connexion directe à un autre ordinateur en utilisant votre port série, parallèle ou votre port infrarouge, ou configure cet ordinateur afin que d'autres ordinateurs puissent s'y connecter.
< Précédent
Suivant >
Annuler

Sélectionnez **Connexion réseau privé virtuel**. Cliquez sur **Suivant**.

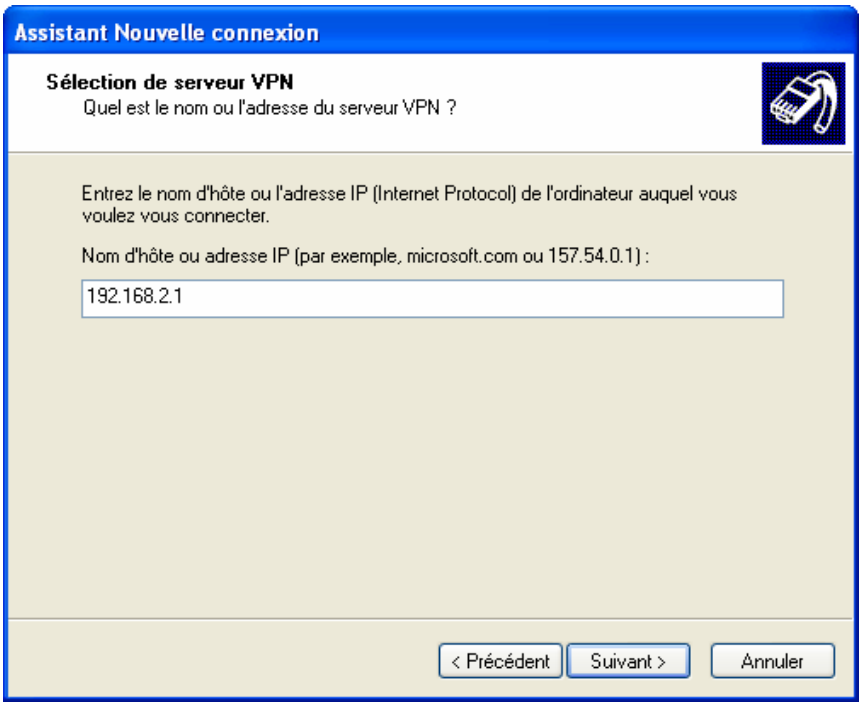

Assistant Nouvelle connexion
Connexion réseau
Comment voulez-vous vous connecter au réseau à votre bureau ?
Crée la connexion suivante :
Connexion d'accès à distance
Permet d'établir une connexion en utilisant un modem et une ligne téléphonique standard ou RNIS.
Connexion réseau privé virtuel
Permet d'établir une connexion réseau en utilisant une connexion réseau privé virtuel (VPN) via Internet.
< Précédent
Suivant >
Annuler

Saisissez le nom de cette connexion dans le champ **Nom de la société**. Cliquez sur **Suivant**.

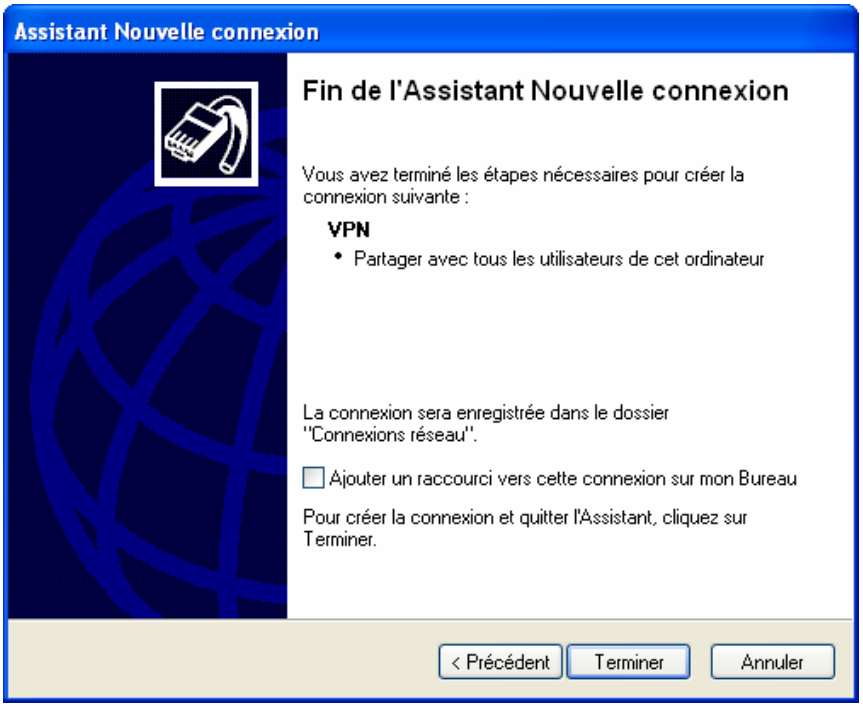

Assistant Nouvelle connexion
Nom de la connexion
Spécifiez un nom pour cette connexion à votre lieu de travail.
Entrez un nom pour cette connexion dans la case suivante.
Nom de la société
VPN
Par exemple, vous pouvez entrer le nom de votre lieu de travail ou le nom du serveur auquel vous allez vous connecter.
< Précédent
Suivant >
Annuler

Entrez ensuite l'adresse IP de l'interface WAN. Si vous utilisez une adresse IP statique pour laquelle vous avez configuré un nom de domaine, ou si vous utilisez une adresse IP dynamique pour laquelle vous avez configuré un nom de domaine via un service de DNS dynamique et que vous avez activé la fonction DNS dynamique du routeur, vous pouvez entrer ce nom de domaine ici. Si votre routeur utilise une adresse IP dynamique, nous vous suggérons d'acquérir un nom de domaine auprès d'un service de DNS dynamique. Ainsi, vous n'aurez pas à modifier la configuration du client PPTP en cas de modification de l'adresse IP de l'interface WAN du routeur.

Saisissez le nom d'hôte ou l'adresse IP de l'interface WAN du routeur dans le champ réservé à cet effet. Cliquez sur **Suivant**.

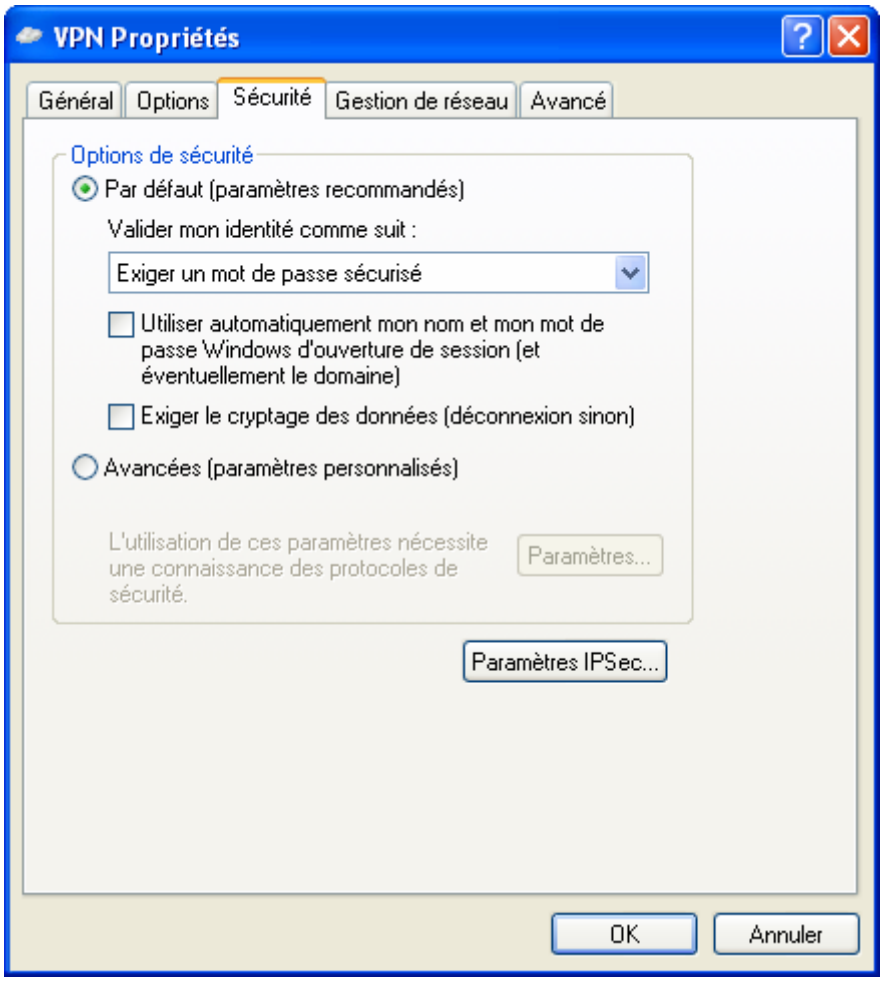

Assistant Nouvelle connexion
Sélection de serveur VPN
Quel est le nom ou l'adresse du serveur VPN ?
Entrez le nom d'hôte ou l'adresse IP (Internet Protocol) de l'ordinateur auquel vous voulez vous connecter.
Nom d'hôte ou adresse IP (par exemple, microsoft.com ou 157.54.0.1) :
192.168.2.1
< Précédent
Suivant >
Annuler

Pour ajouter un raccourci vers cette connexion sur votre Bureau, cochez la case correspondante. Cliquez sur **Terminer**.


Assistant Nouvelle connexion
Fin de l'Assistant Nouvelle connexion
Vous avez terminé les étapes nécessaires pour créer la connexion suivante :
VPN
• Partager avec tous les utilisateurs de cet ordinateur
La connexion sera enregistrée dans le dossier "Connexions réseau".
Ajouter un raccourci vers cette connexion sur mon Bureau
Pour créer la connexion et quitter l'Assistant, cliquez sur Terminer.
< Précédent
Terminer
Annuler

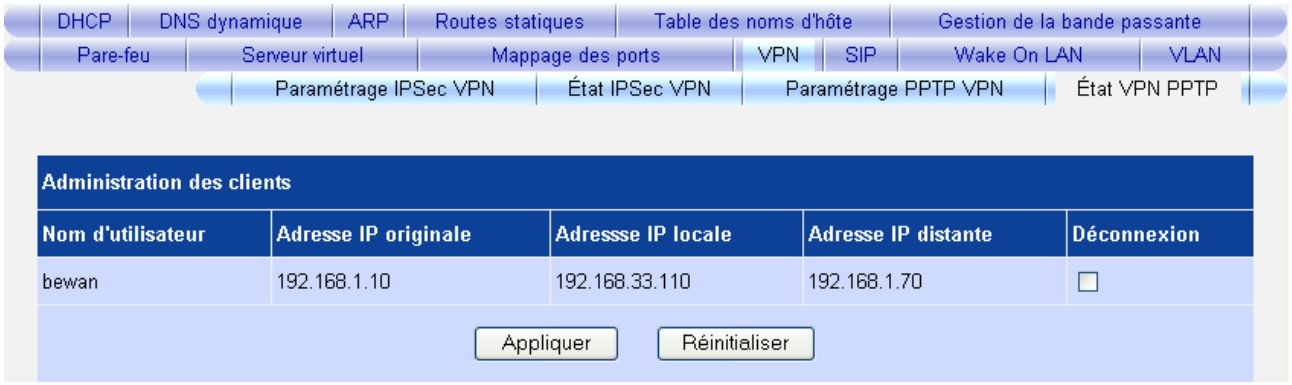
Cliquez sur le bouton **Propriétés** avant de vous connecter.

Décochez l'option **Exiger le cryptage des données (déconnexion sinon)**. Cliquez sur **OK**.



Entrez ensuite votre **Nom d'utilisateur** et votre **Mot de passe** PPTP. Cliquez sur **Se connecter**.

Windows vous informe lorsque la connexion a été établie avec succès. Si vous ouvrez la page de configuration **État VPN PPTP** du routeur, la connexion PPTP active s'affiche.

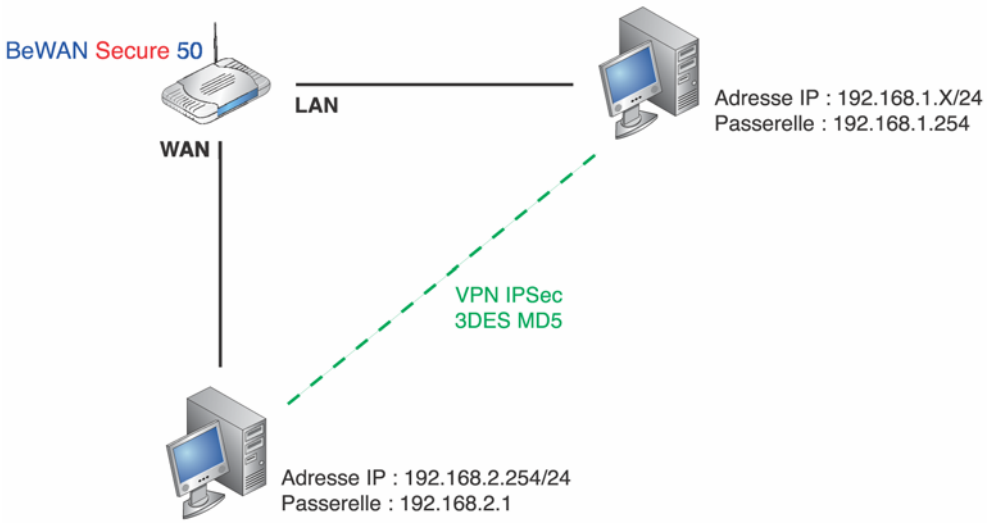


Pour mettre fin à la connexion PPTP, cochez la case **Déconnexion** correspondante et cliquez sur le bouton **Appliquer**. Cliquez sur le bouton **Réinitialiser** pour annuler la sélection de la case **Déconnexion**.

*Pour le paramétrage PPTP de base, nous vous suggérons de choisir une adresse IP privée (non publique) telle que 10.X.X.X, 172.X.X.X ou 192.X.X.X qui n'entrera pas en conflit avec l'**Adresse IP distante** et l'adresse IP de l'interface LAN pour l'**Adresse IP locale**. Nous vous suggérons également d'utiliser pour l'**Adresse IP distante** le même sous-réseau que celui de l'interface LAN du routeur. Sinon, ce dernier doit être la passerelle par défaut du réseau local.*

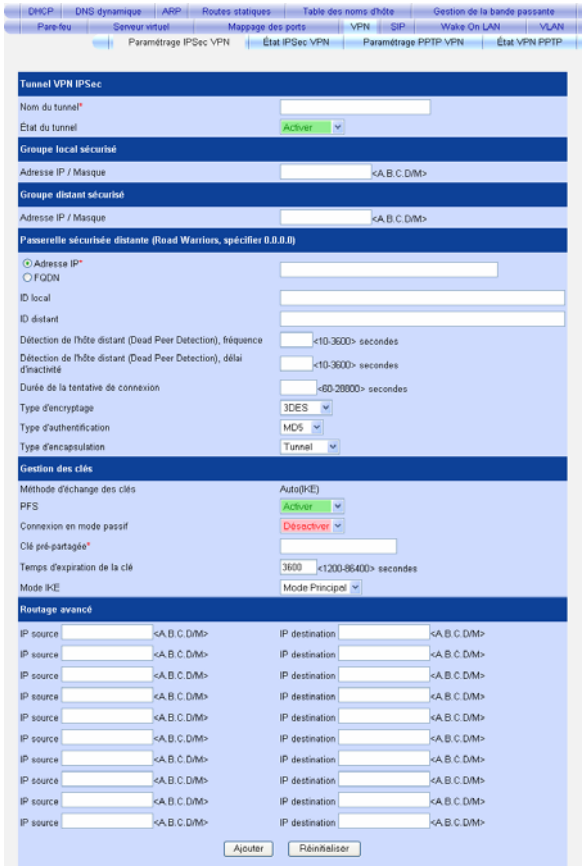
PARAMETRAGE IPSEC VPN

Le protocole VPN IPSec permet la tunnellisation, l'authentification et le cryptage des données. Il protège les données sensibles transmises sur les réseaux publics. L'exemple ci-dessous illustre l'établissement d'une connexion VPN IPSec entre le routeur et Windows XP.

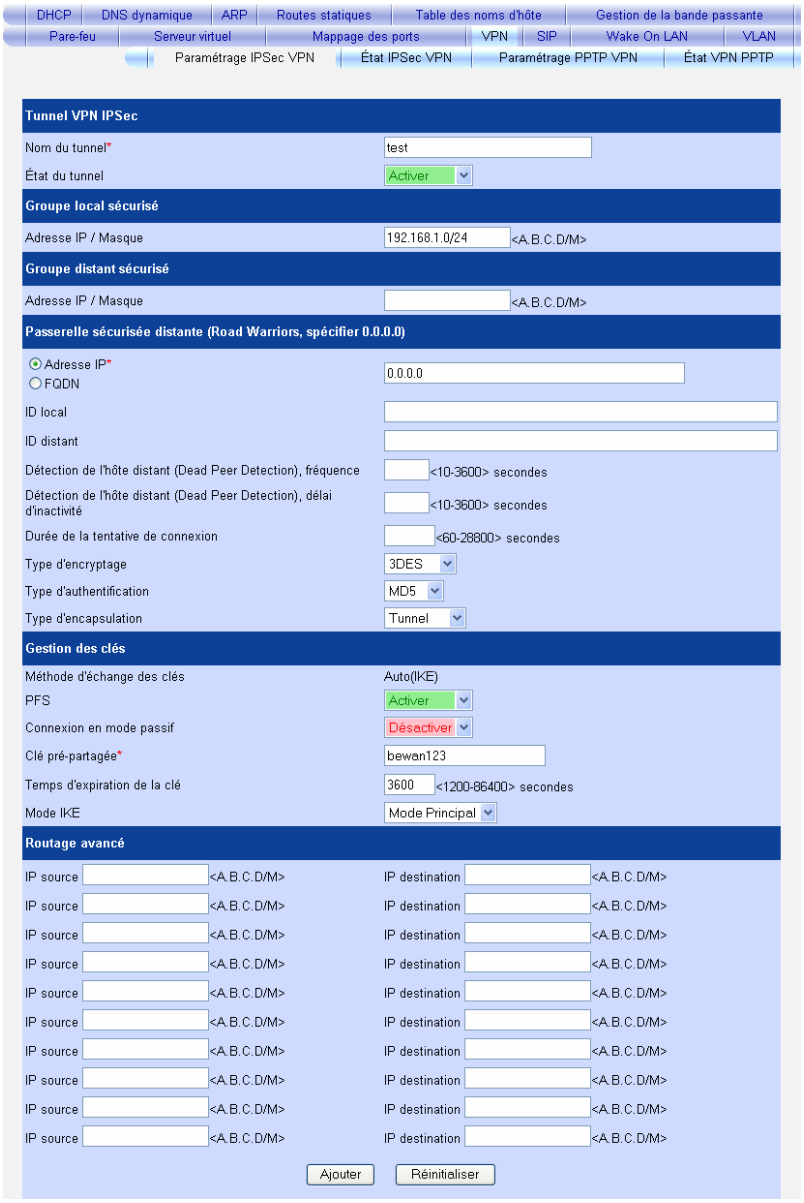


Veuillez considérer l'illustration ci-dessus. L'adresse IP du Windows XP est 192.168.2.254. Celle de la passerelle par défaut du système de réseau 192.168.1.0/24 est 192.168.1.254/24. Ces deux systèmes établissent une connexion VPN entre eux.

Cliquez sur **VPN**, puis dans **Paramétrage IPSec VPN**, configurez les paramètres du tunnel VPN IPSec.



Saisissez ensuite les valeurs indiquées sur la capture d'écran ci-dessous.



Nom du tunnel

Le nom de ce tunnel (obligatoire).

Groupe local sécurisé

Si vous souhaitez établir la connexion VPN IPSec entre le sous-réseau local et un sous-réseau/hôte distant, entrez ici le sous-réseau IP local.

Groupe distant sécurisé

Si vous souhaitez établir la connexion VPN IPSec entre ce système ou le sous-réseau local et un sous-réseau distant, entrez ici le sous-réseau IP distant.

Passerelle sécurisée distante

Si vous souhaitez établir la connexion VPN IPSec avec un hôte distant, entrez l'adresse IP Internet de cet hôte ; pour établir la connexion VPN IPSec avec un sous-réseau distant, entrez l'adresse IP Internet de la passerelle sécurisée IPSec distante.

ID local

Permet d'indiquer explicitement l'ID de l'hôte local.

ID distant

Permet d'indiquer explicitement l'ID de l'hôte distant.

Détection de l'hôte distant, fréquence

L'intervalle de temps est exprimé en secondes. Ce paramètre définit la fréquence à laquelle le routeur envoie un paquet pour contrôler l'état du tunnel IPSec.

Détection de l'hôte distant, délai d'inactivité

L'intervalle de temps est exprimé en secondes. Ce paramètre définit la durée pendant laquelle le routeur attend la réponse du routeur VPN distant avant de ré-établir la connexion IPSec. Cette valeur doit être supérieure à celle de la fréquence.

Type d'encryptage

L'algorithme de cryptage utilisé. La norme 3DES (Triple Data Encryption Standard) est désormais prise en charge.

Type d'authentification

L'algorithme d'authentification utilisé pour vérifier l'intégrité des données (si elles sont interpolées ou non). Le système prend en charge deux algorithmes d'authentification : MD-5 et SHA-1.

Type d'encapsulation

Si l'une des extrémités (ou les deux) entre lesquelles la connexion VPN IPSec est établie est un sous-réseau, sélectionnez **Tunnel**. Si les deux extrémités sont des hôtes, vous pouvez sélectionner **Tunnel** ou **Transport**. Bien que le mode **Tunnel** engendre un surdébit plus important que le mode **Transport**, il offre une meilleure compatibilité.

Méthode d'échange des clés

Le système prend en charge le protocole IKE (***I**nternet **K**ey **E**xchange*).

PFS

Acronyme de Perfect Forward Secrecy (confidentialité de transmission parfaite).

Clé pré-partagée

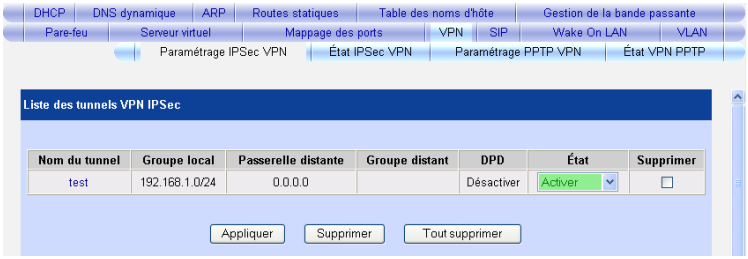
Les deux extrémités d'un tunnel VPN IPSec doivent utiliser la même clé pré-partagée.

Temps d'expiration de la clé

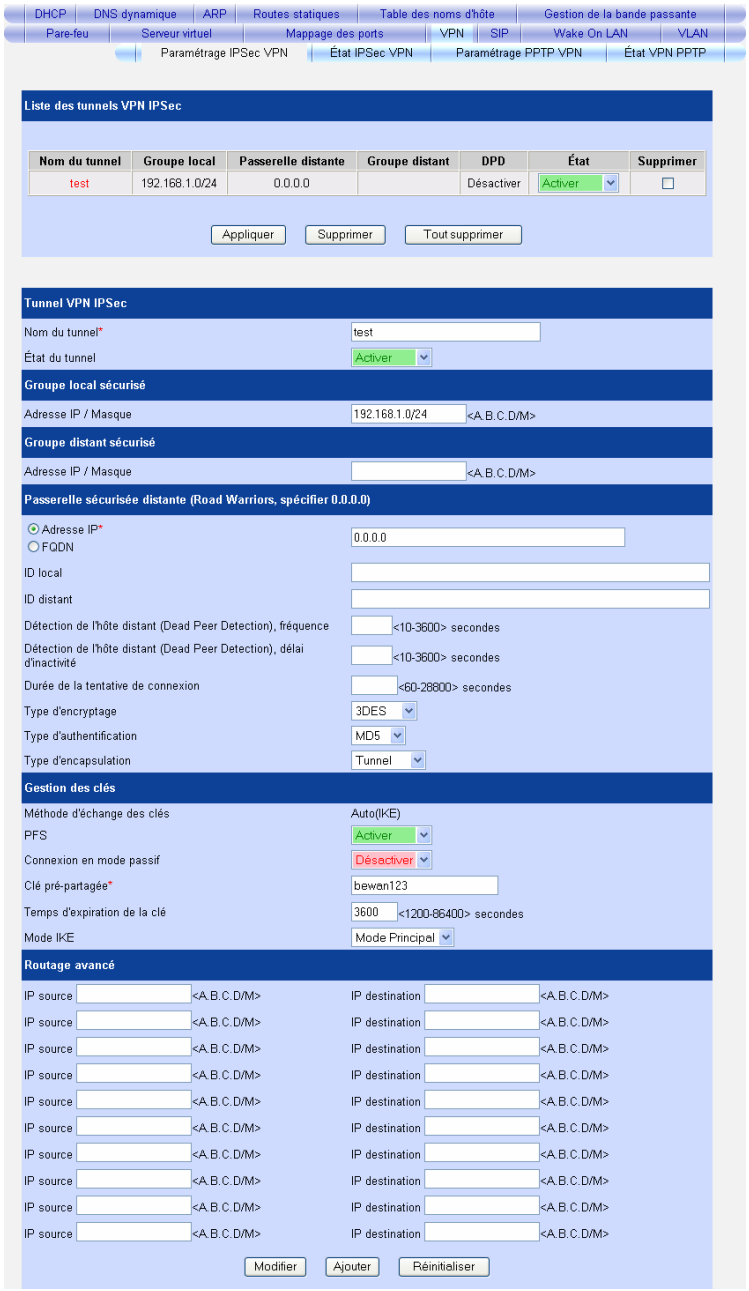
Durée de vie de la clé d'authentification et de cryptage. Lorsque la durée de la connexion VPN IPSec dépasse le temps indiqué, une nouvelle clé d'authentification et de cryptage est générée et les clés sont échangées. Les informations relatives à la connexion VPN IPSec modifiée sont également actualisées en conséquence.

Lorsque vous cliquez sur le bouton **Ajouter** pour valider le paramétrage, l'écran affiche le tunnel VPN IPSec actuellement configuré. Si vous cliquez sur **Réinitialiser**, toutes les valeurs de paramétrage saisies seront effacées.

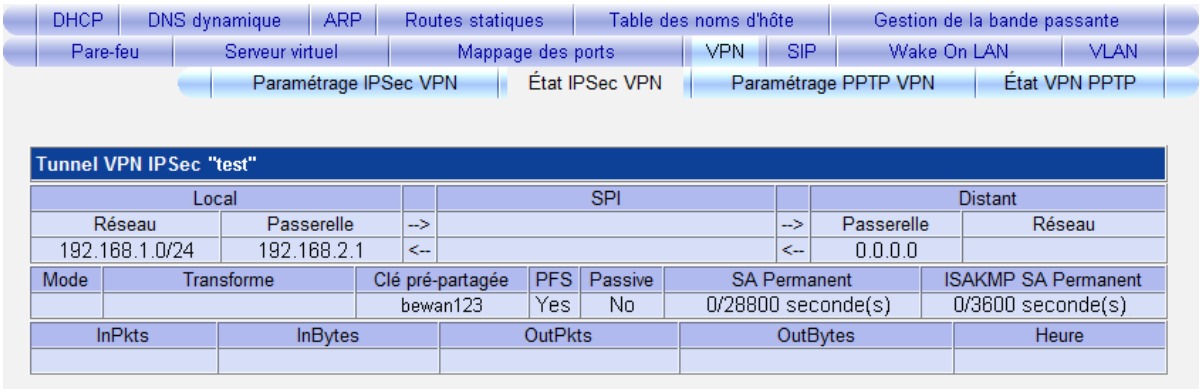
Pour supprimer ou modifier une configuration de tunnel, cliquez sur le nom du tunnel à supprimer ou à modifier. L'écran de suppression/modification ci-dessous s'affiche.



Cet écran est similaire à celui permettant d'ajouter un tunnel VPN, à ceci près que le bouton **Ajouter** est remplacé par le bouton **Modifier** et que l'utilisateur modifie les paramètres de la connexion VPN IPSec. Après avoir modifié les valeurs de paramétrage, cliquez sur le bouton **Modifier** pour que les modifications soient prises en compte. Pour supprimer un tunnel VPN, cliquez sur le bouton **Supprimer**, ou cliquez sur le bouton **Tout supprimer** pour supprimer tous les tunnels.

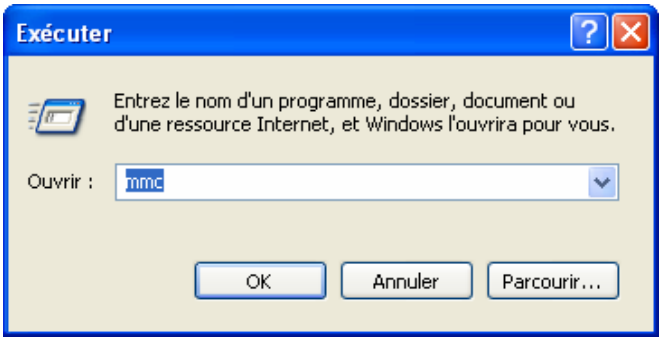


Cliquez sur le bouton **État IPSec VPN** pour afficher toutes les valeurs de paramétrage et tous les états du tunnel VPN. La capture d'écran ci-dessous présente le seul tunnel VPN configuré pour le moment.

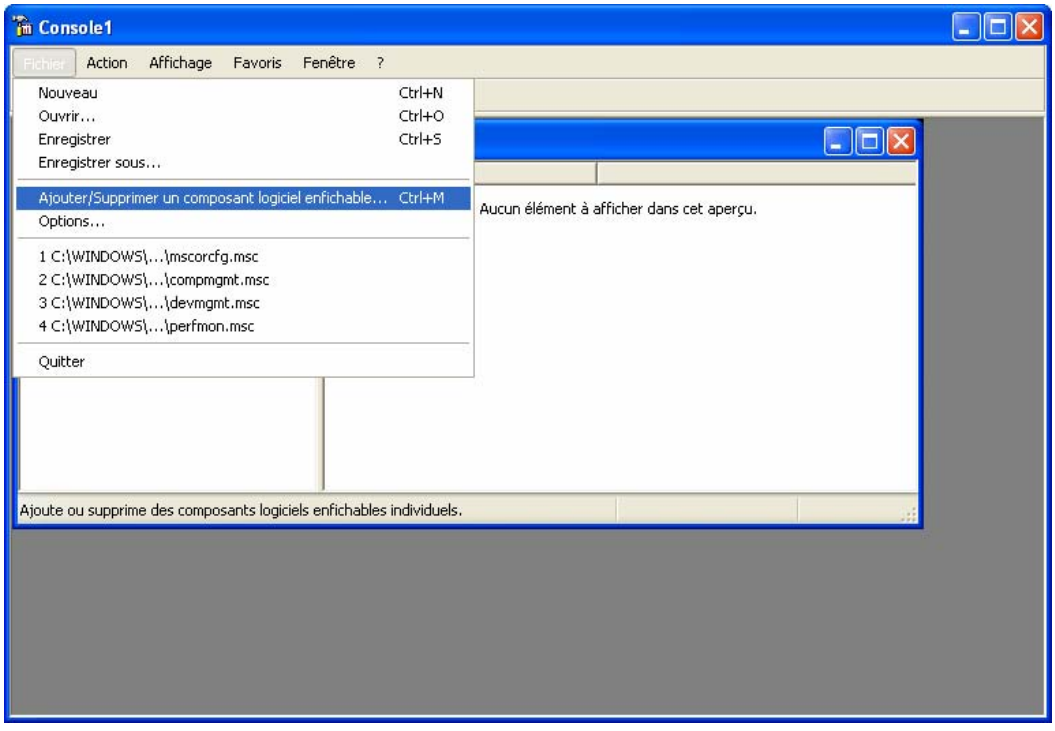


Dans la suite, nous allons présenter comment créer un tunnel VPN avec ce système à l'aide de l'hôte Windows XP.

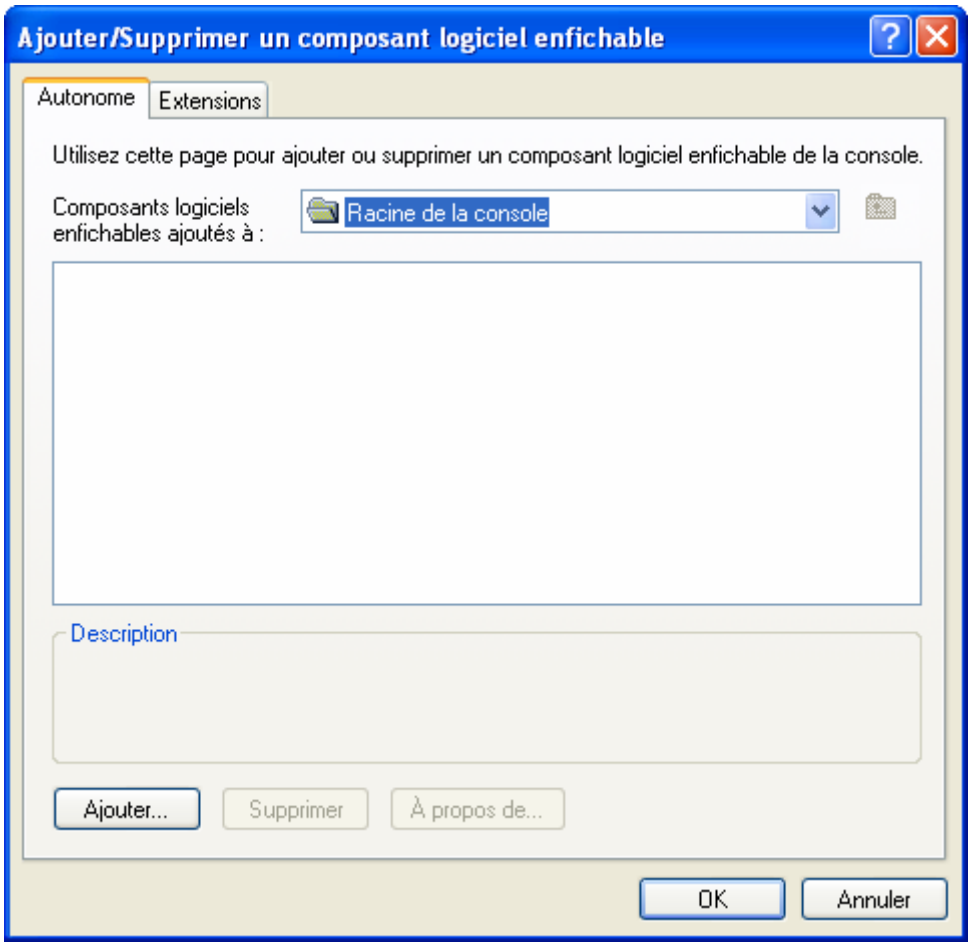
Cliquez sur la commande **Exécuter** du menu **Démarrer**. Saisissez **mmc** dans la zone de texte **Ouvrir**. Cliquez sur le bouton **OK**.



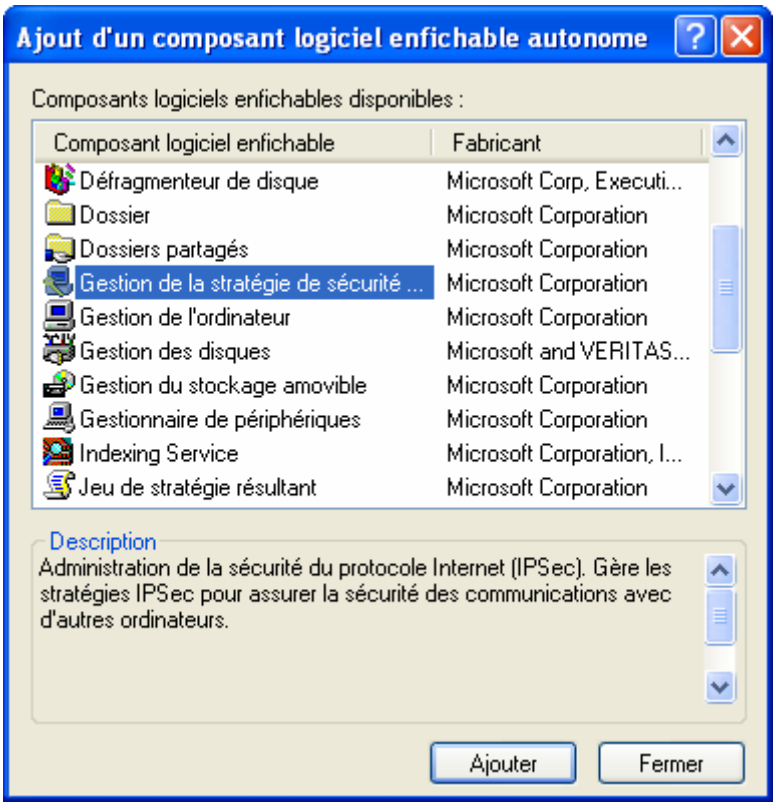
Cliquez sur **Ajouter/Supprimer un composant logiciel enfichable…** dans le menu **Fichier**.



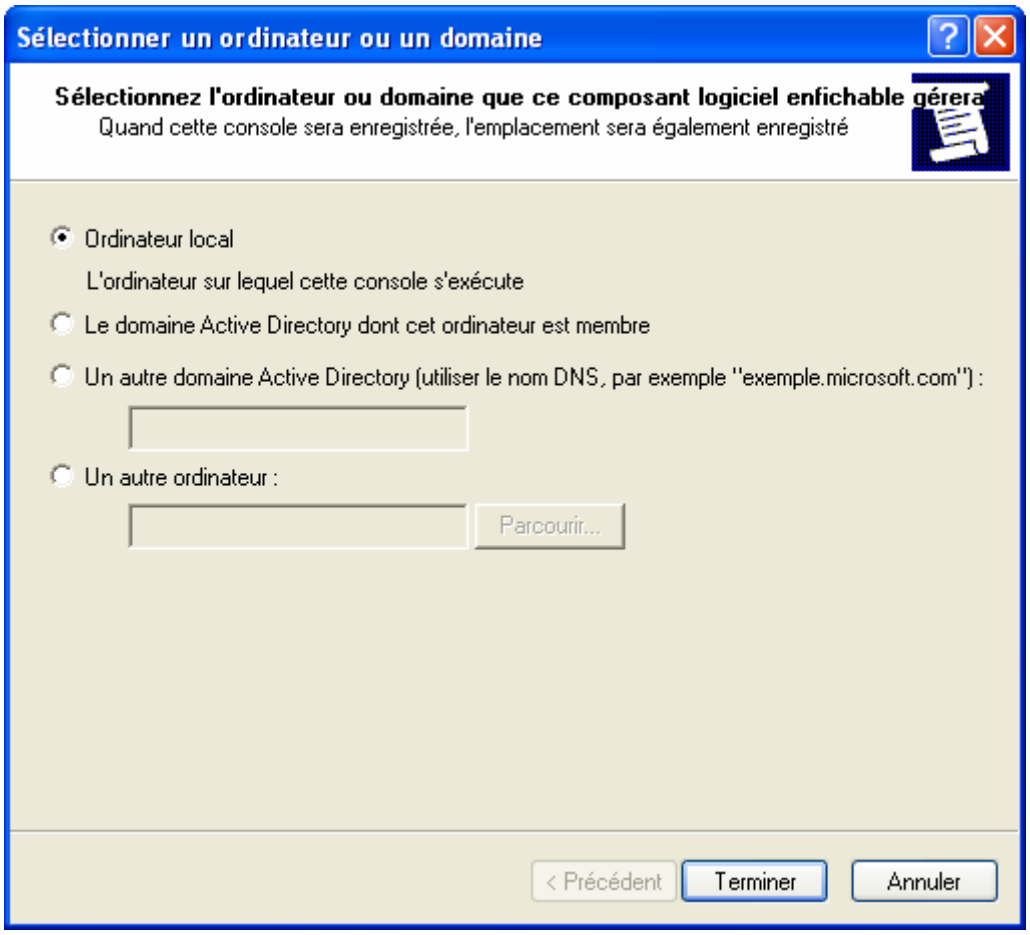
Cliquez sur le bouton **Ajouter…**.



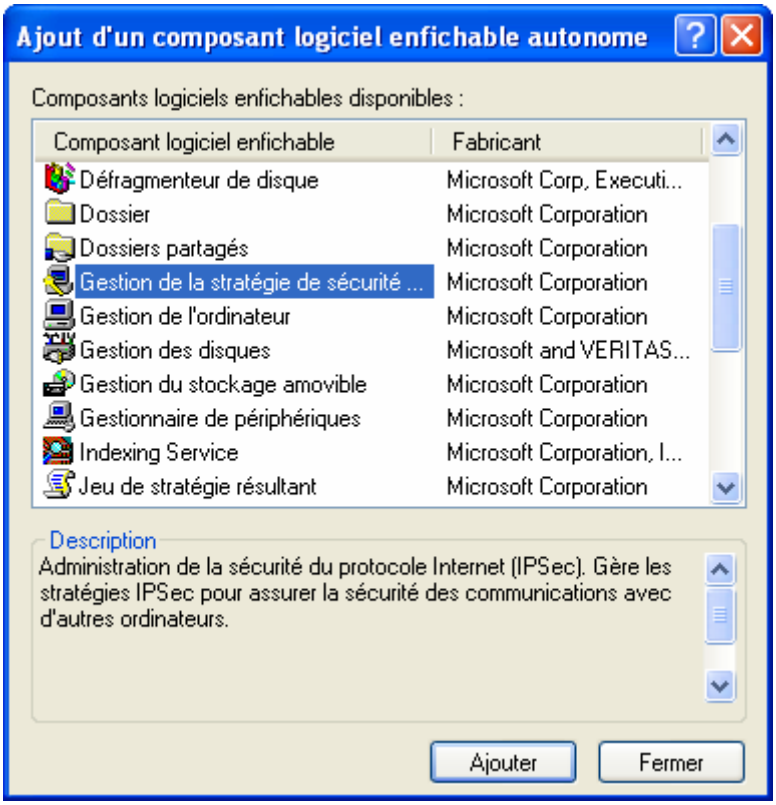
Cliquez sur **Gestion de la stratégie de sécurité du protocole IP**. Cliquez sur le bouton **Ajouter**.



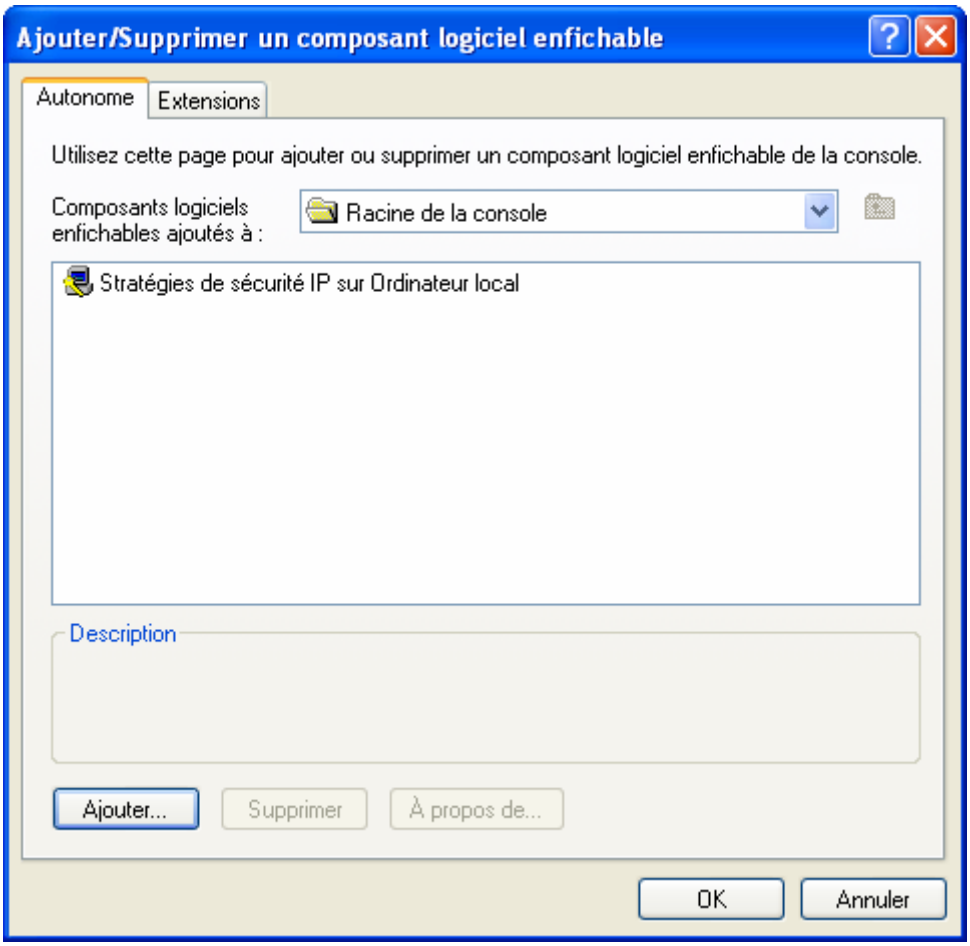
Sélectionnez **Ordinateur local**. Cliquez sur le bouton **Terminer**.


Sélectionner un ordinateur ou un domaine
Sélectionnez l'ordinateur ou domaine que ce composant logiciel enfichable gérera
Quand cette console sera enregistrée, l'emplacement sera également enregistré
Ordinateur local
L'ordinateur sur lequel cette console s'exécute
Le domaine Active Directory dont cet ordinateur est membre
Un autre domaine Active Directory (utiliser le nom DNS, par exemple "exemple.microsoft.com") :
Un autre ordinateur :
Parcourir...
< Précédent
Terminer
Annuler

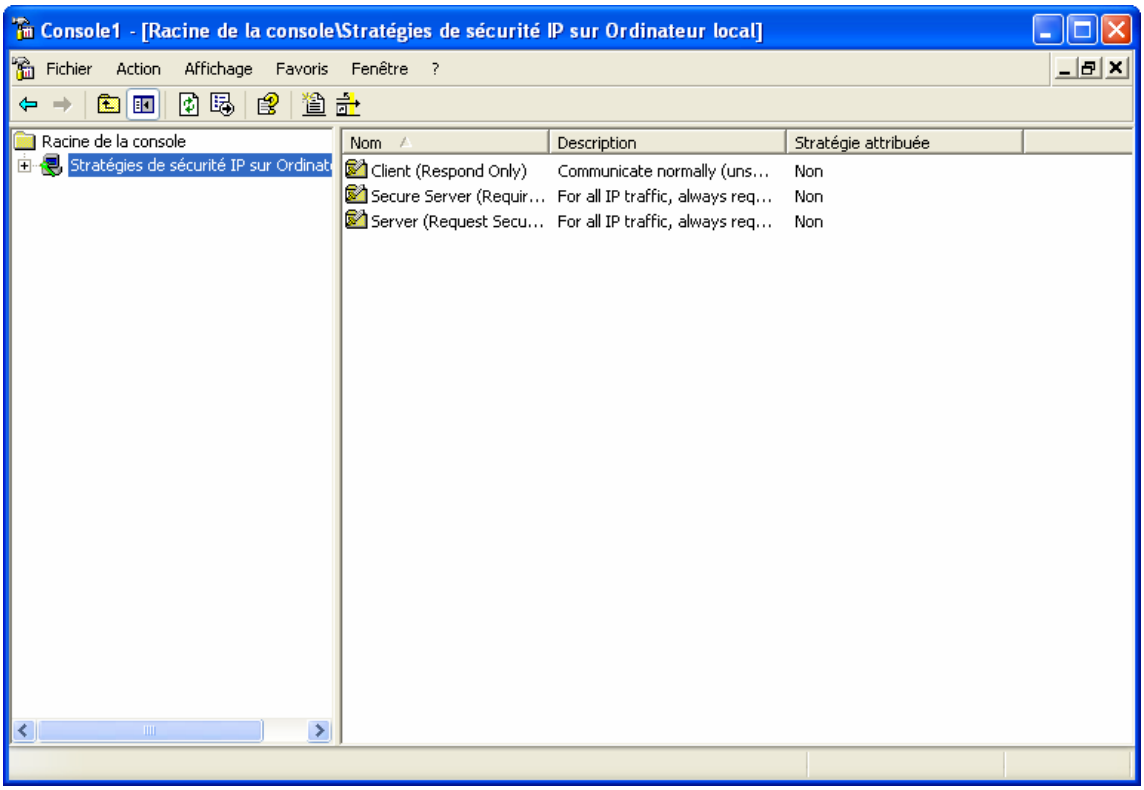
Cliquez sur le bouton **Fermer**.



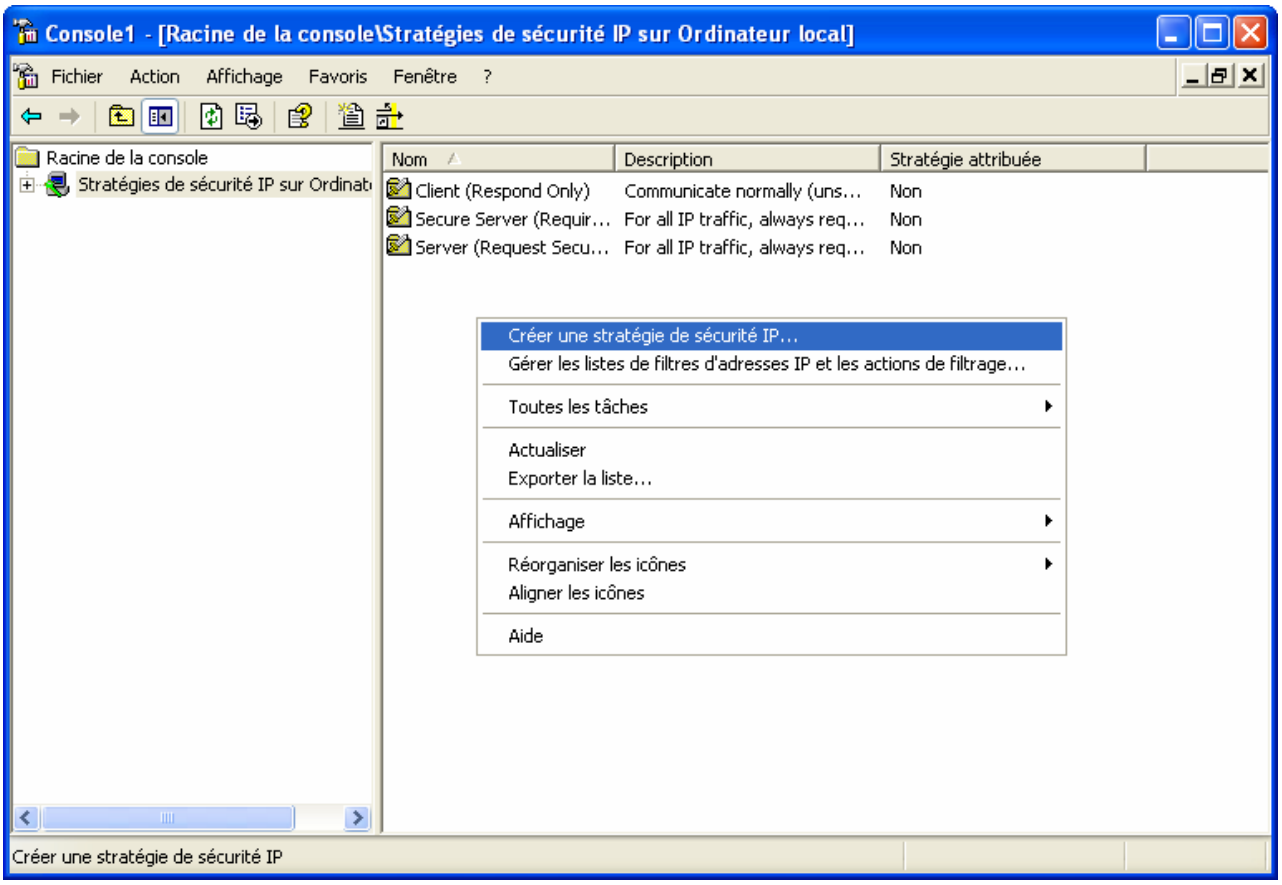
Cliquez sur le bouton **OK**.



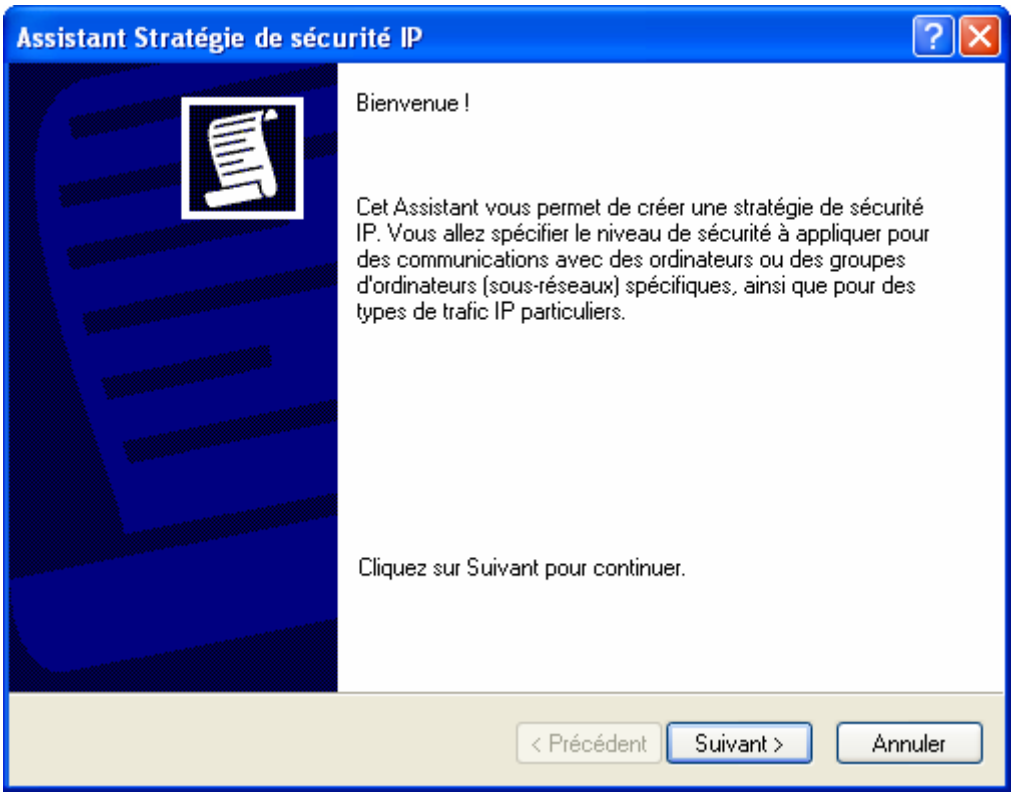
Cliquez sur **Stratégies de sécurité IP sur Ordinateur local**.



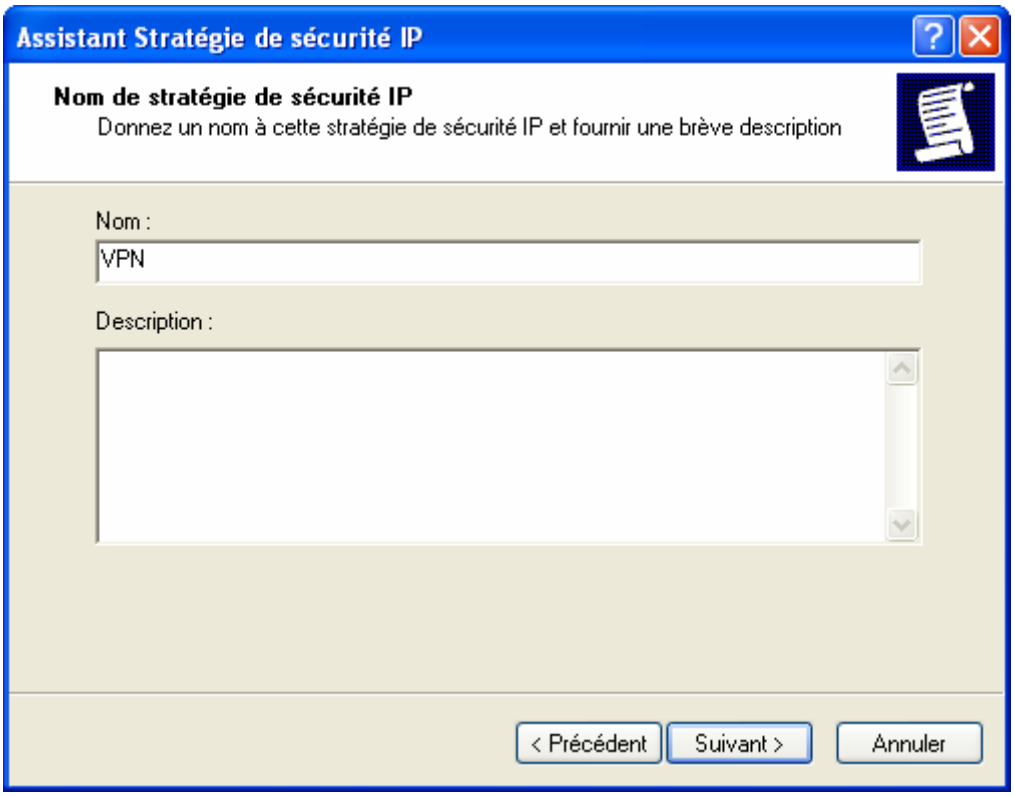
Cliquez avec le bouton droit de la souris sur un espace vide de la fenêtre de droite. Sélectionnez **Créer une stratégie de sécurité IP…**.



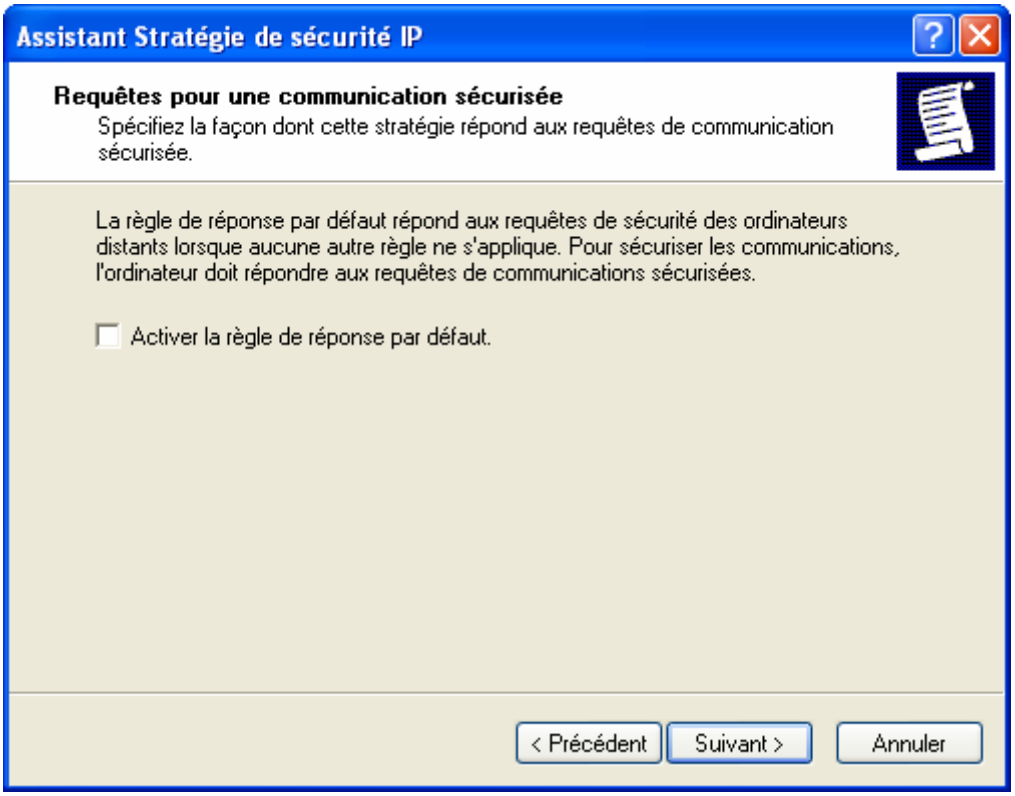
Cliquez sur le bouton **Suivant**.


Assistant Stratégie de sécurité IP
Bienvenue !
Cet Assistant vous permet de créer une stratégie de sécurité IP. Vous allez spécifier le niveau de sécurité à appliquer pour des communications avec des ordinateurs ou des groupes d'ordinateurs (sous-réseaux) spécifiques, ainsi que pour des types de trafic IP particuliers.
Cliquez sur Suivant pour continuer.
< Précédent
Suivant >
Annuler

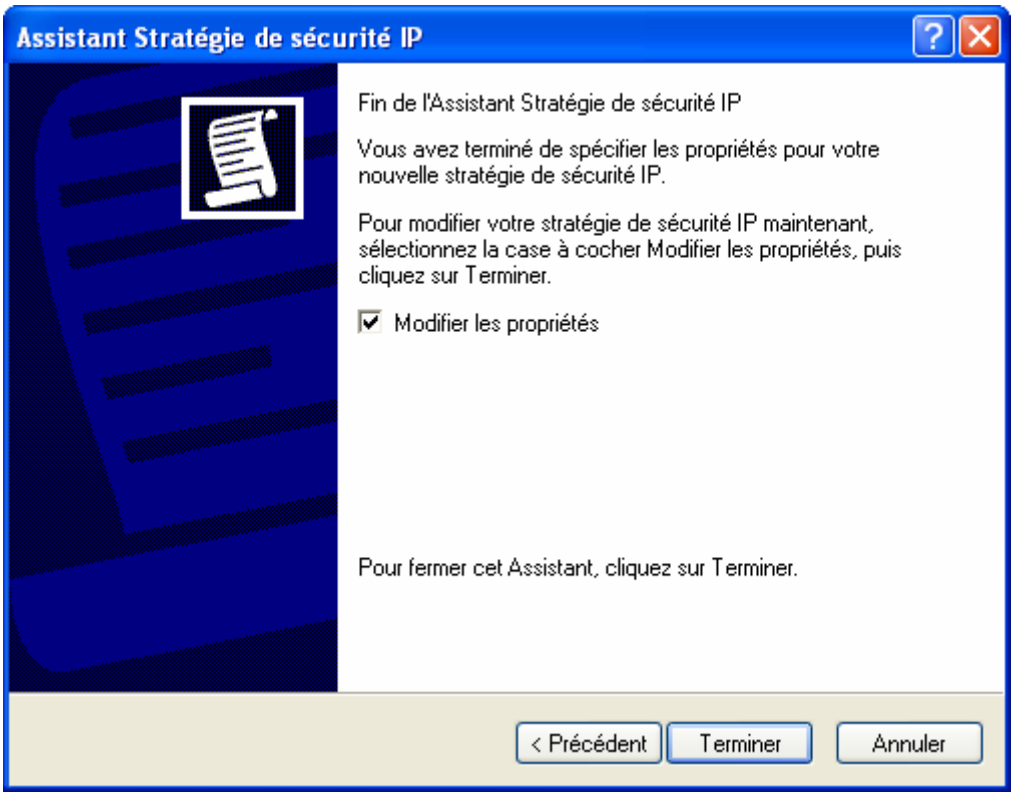
Tapez ***VPN*** dans le champ **Nom**.


Assistant Stratégie de sécurité IP
Nom de stratégie de sécurité IP
Donnez un nom à cette stratégie de sécurité IP et fournir une brève description
Nom :
VPN
Description :
< Précédent
Suivant >
Annuler

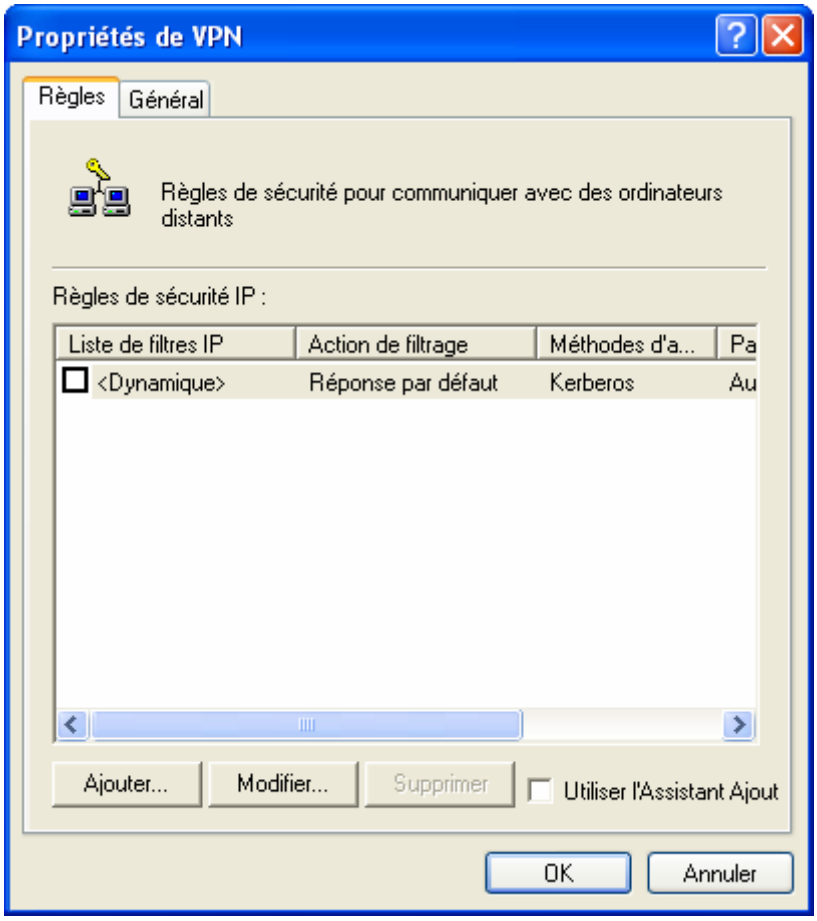
Décochez la case **Activer la règle de réponse par défaut**. Cliquez sur le bouton **Suivant**.


Assistant Stratégie de sécurité IP
Requêtes pour une communication sécurisée
Spécifiez la façon dont cette stratégie répond aux requêtes de communication sécurisée.
La règle de réponse par défaut répond aux requêtes de sécurité des ordinateurs distants lorsque aucune autre règle ne s'applique. Pour sécuriser les communications, l'ordinateur doit répondre aux requêtes de communications sécurisées.
Activer la règle de réponse par défaut.
< Précédent
Suivant >
Annuler

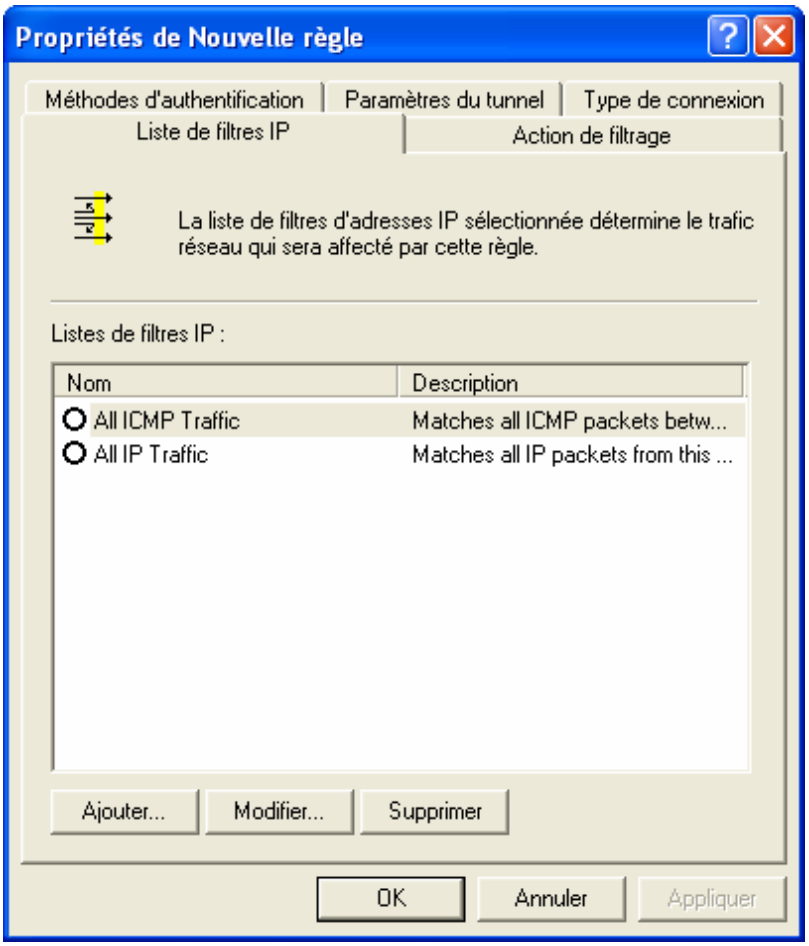
Cochez la case **Modifier les propriétés**. Cliquez sur le bouton **Terminer**.


Assistant Stratégie de sécurité IP
Fin de l'Assistant Stratégie de sécurité IP
Vous avez terminé de spécifier les propriétés pour votre nouvelle stratégie de sécurité IP.
Pour modifier votre stratégie de sécurité IP maintenant, sélectionnez la case à cocher Modifier les propriétés, puis cliquez sur Terminer.
Modifier les propriétés
Pour fermer cet Assistant, cliquez sur Terminer.
< Précédent
Terminer
Annuler

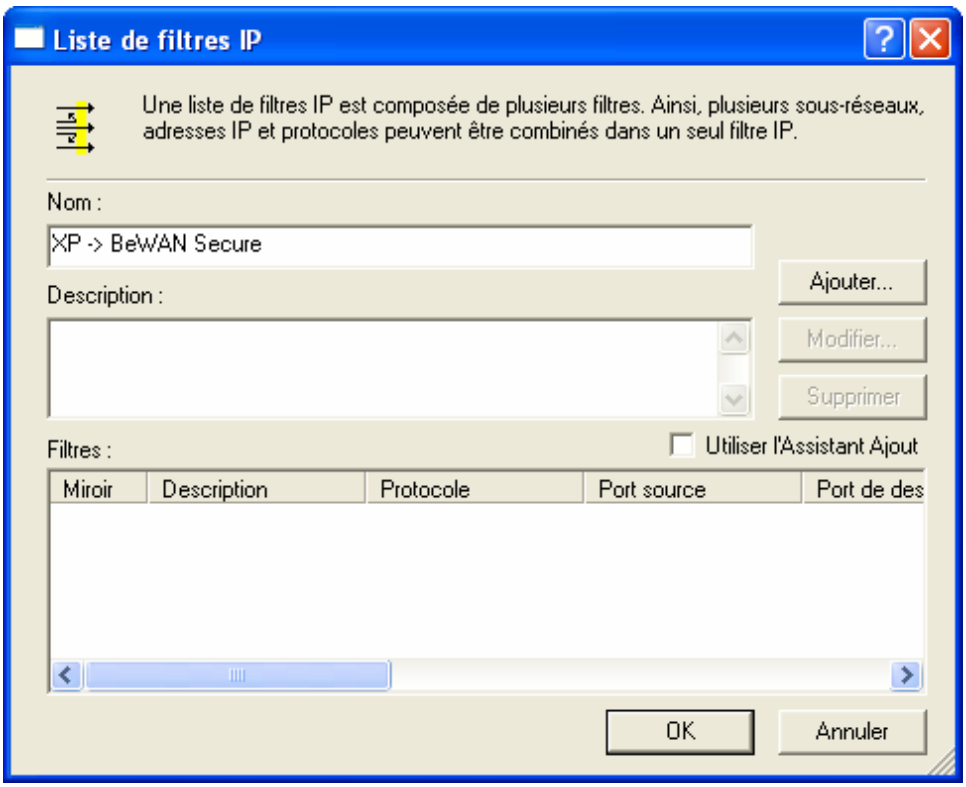
Décochez la case **Utiliser l'Assistant Ajout**. Cliquez sur le bouton **Ajouter…**.



Cliquez sur le bouton **Ajouter…**.



Saisissez le nom de la liste de filtres IP (***XP -> BeWAN Secure*** dans notre cas). Cliquez sur **Ajouter…**.

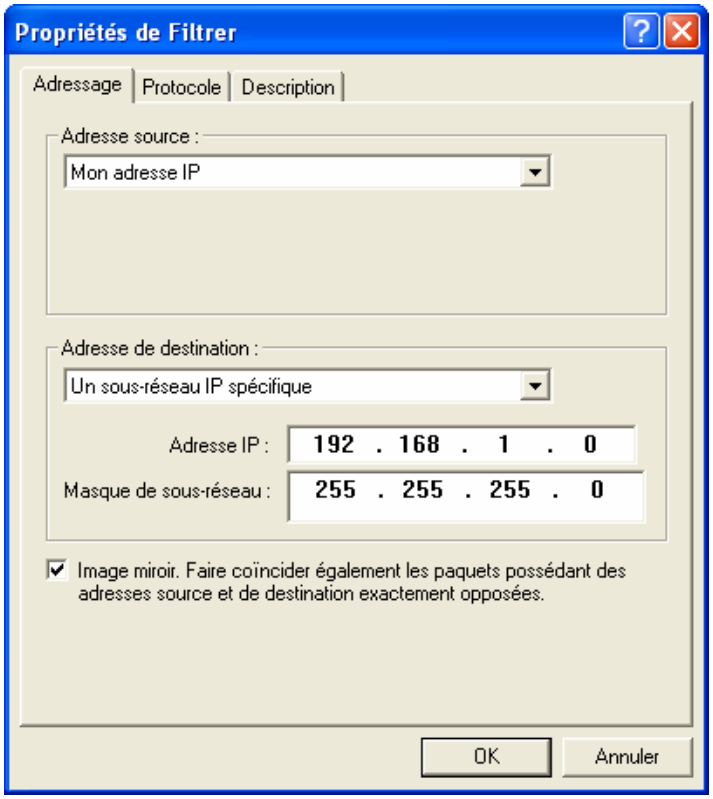


Sélectionnez **Mon adresse IP** dans la liste déroulante **Adresse source**.

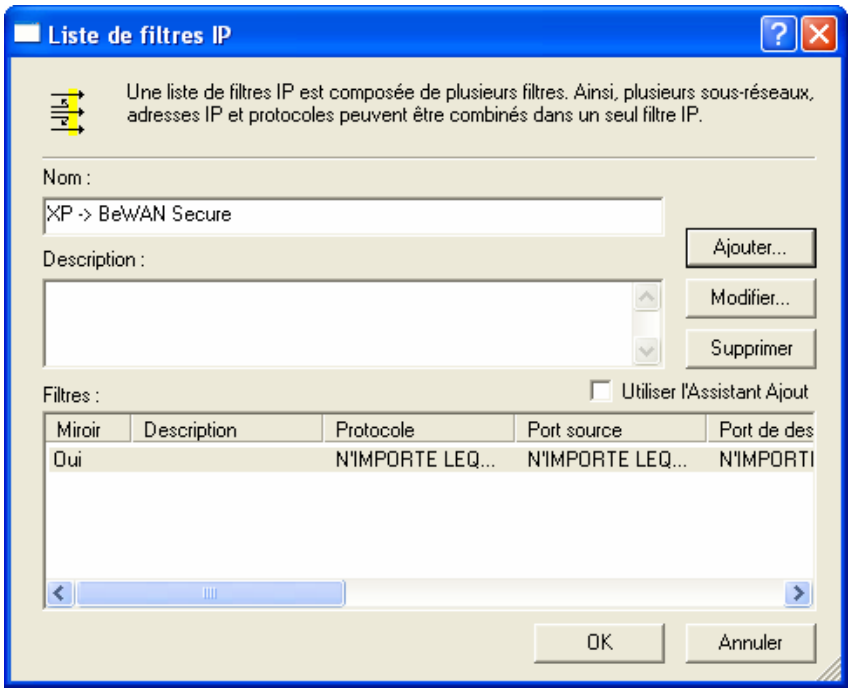
Dans la liste déroulante **Adresse de destination**, sélectionnez **Un sous-réseau IP spécifique**. Entrez le sous-réseau de l'extrémité opposée du tunnel VPN dans les champs **Adresse IP** et **Masque de sous-réseau**. (192.168.1.0/255.255. 255.0)

Cochez la case Image miroir. Faire coïncider également les paquets possédant des adresses source et de destination exactement opposées.

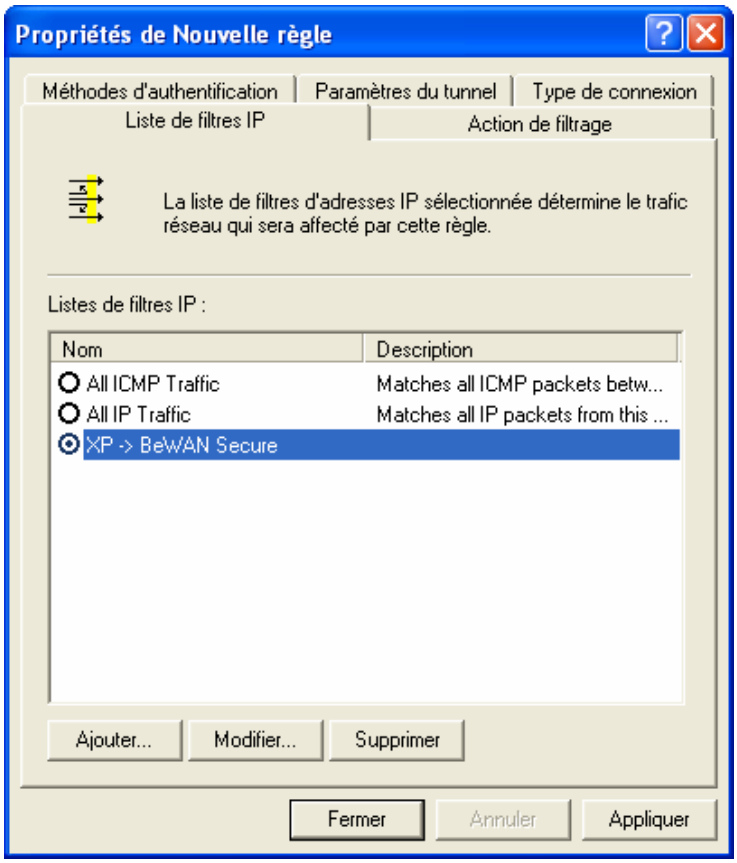
Cliquez sur **OK**.



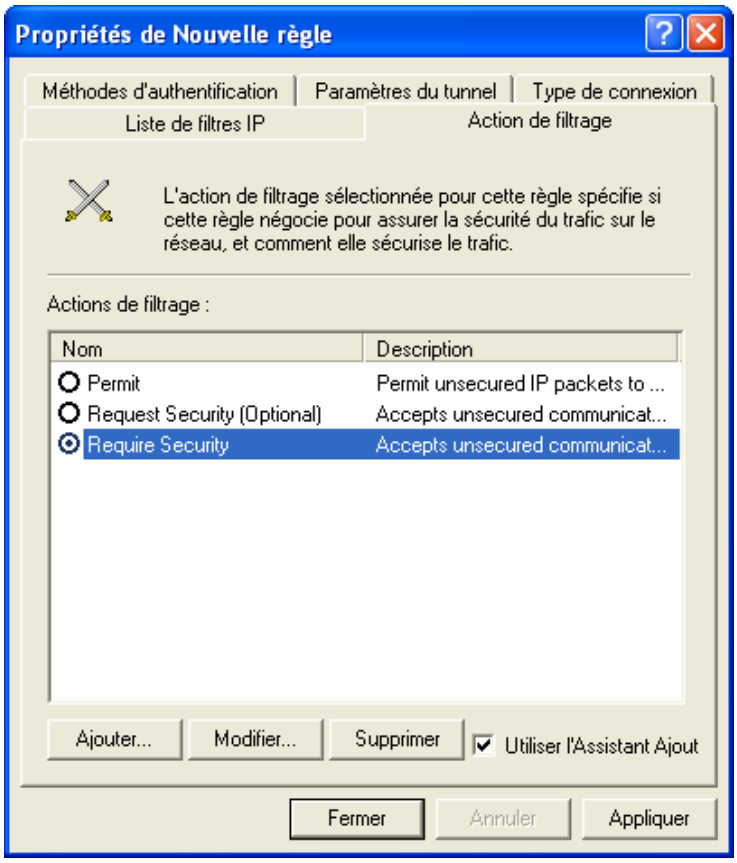
Cliquez sur **OK**. Retournez à la dernière couche.



Sélectionnez la **Liste de filtres IP** précédemment définie (***XP -> BeWAN Secure***). Cliquez sur l'onglet **Action de filtrage**.



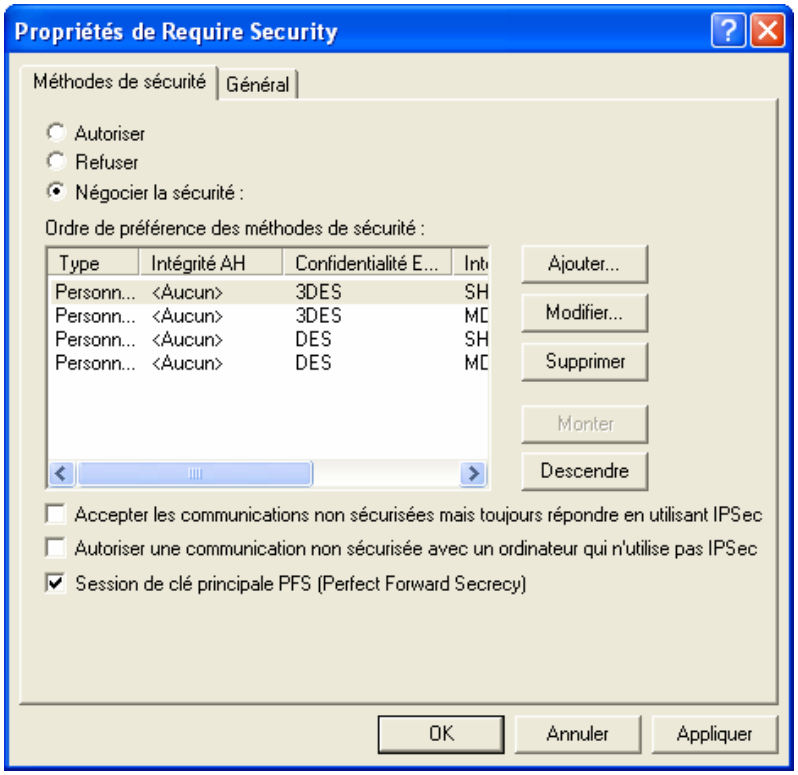
Cliquez sur **Require Security**. Cliquez sur **Modifier…**.



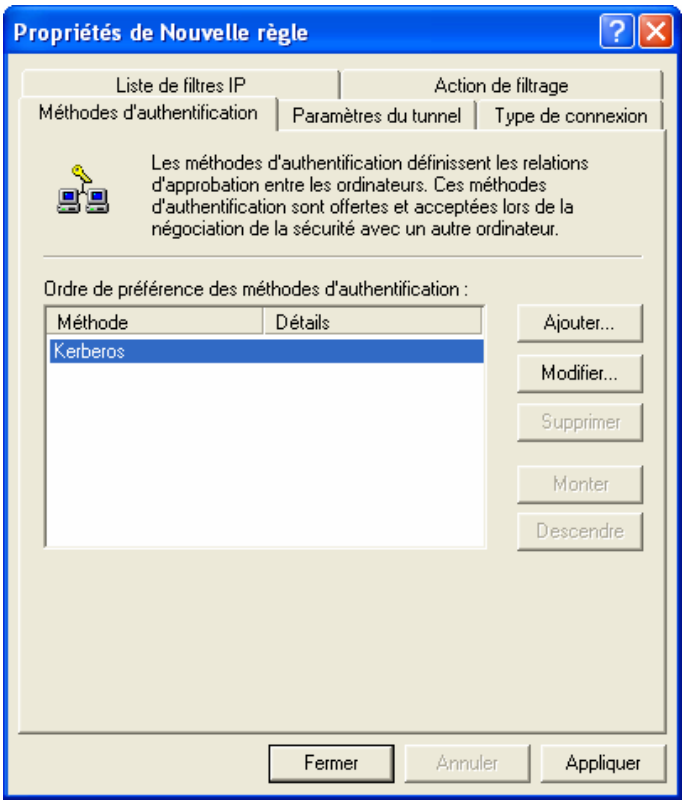
Sélectionnez **Négocier la sécurité**. Vérifiez que les méthodes 3DES/SHA1 et 3DES/MD5 sont prises en charge.

Décochez la case Accepter les communications non sécurisées mais toujours répondre en utilisant IPSec. Cochez la case Session de clé principale PFS (Perfect Forward Secrecy).

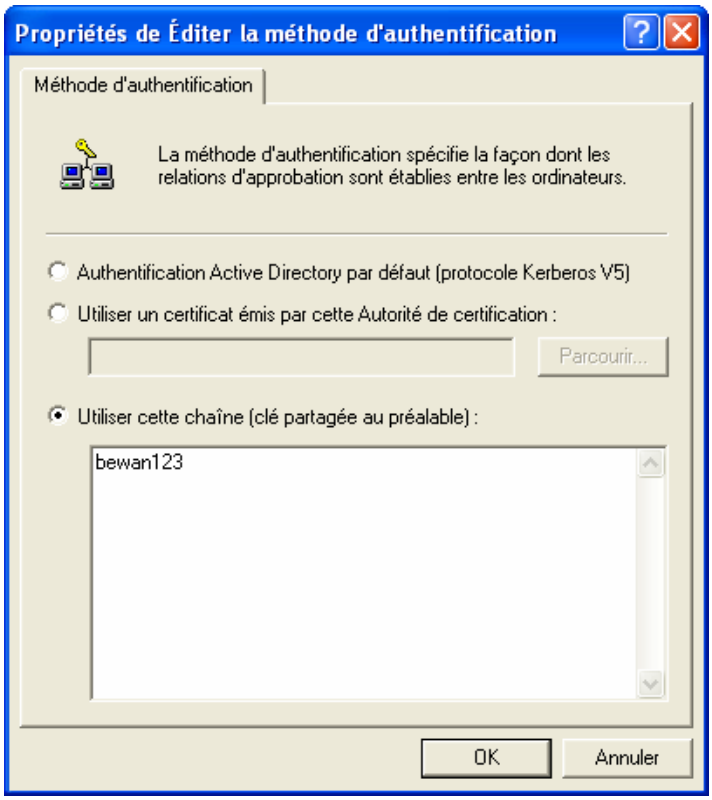
Cliquez sur le bouton **OK**.



Cliquez sur **Modifier…**.

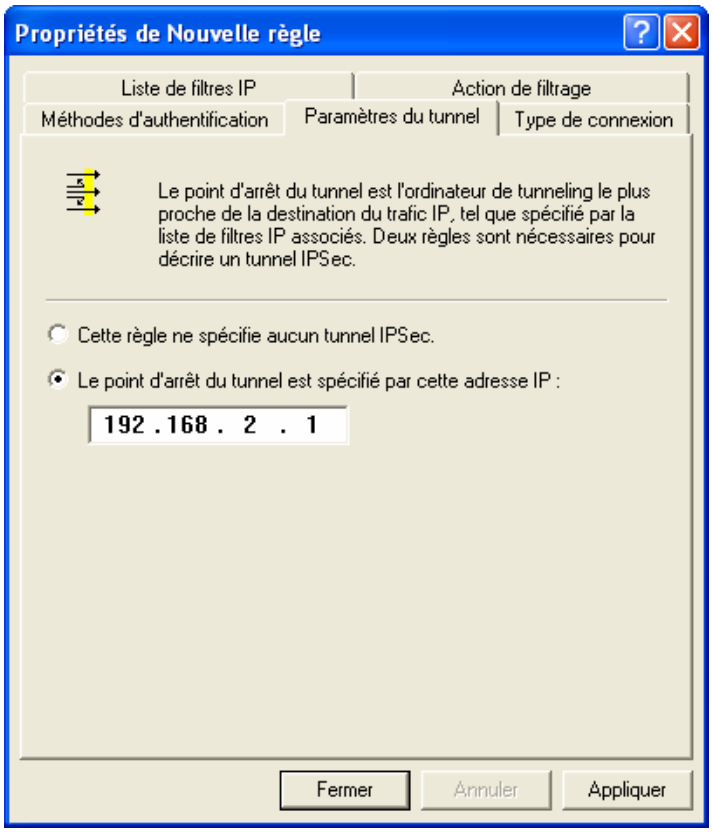


Sélectionnez **Utiliser cette chaîne (clé partagée au préalable)**. Saisissez la clé prédéfinie : ***bewan123***. Cliquez sur **OK**.

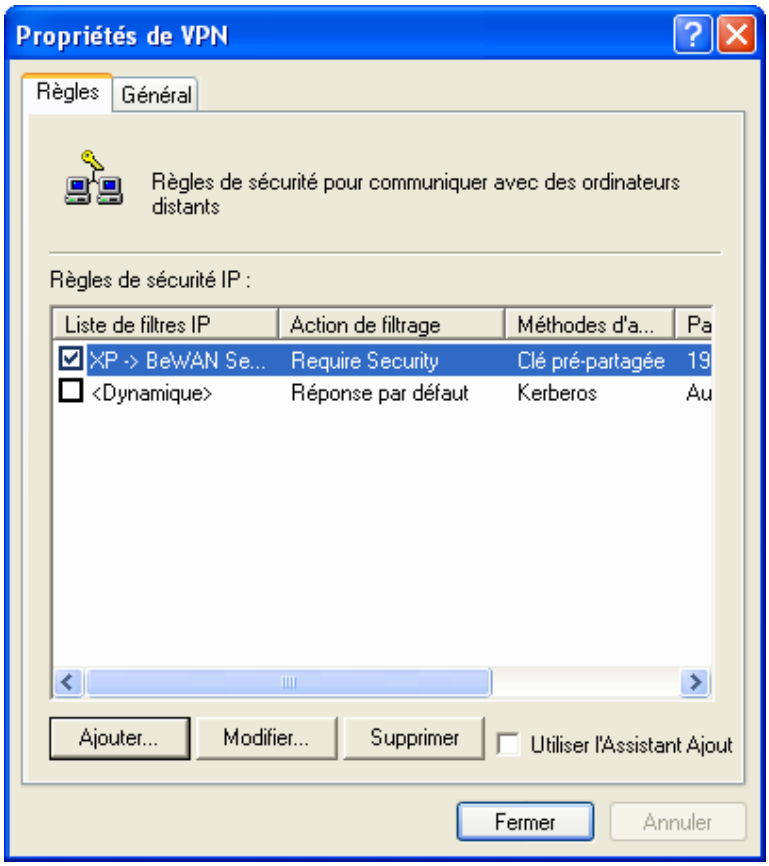

Propriétés de Éditer la méthode d'authentification
Méthode d'authentification
La méthode d'authentification spécifie la façon dont les relations d'approbation sont établies entre les ordinateurs.
Authentification Active Directory par défaut (protocole Kerberos V5)
Utiliser un certificat émis par cette Autorité de certification :
Parcourir...
Utiliser cette chaîne (clé partagée au préalable) :
bewan123
OK
Annuler

Sélectionnez **Le point d'arrêt du tunnel est spécifié par cette adresse IP**. Saisissez l'adresse IP de l'interface WAN de l'extrémité opposée du tunnel VPN.

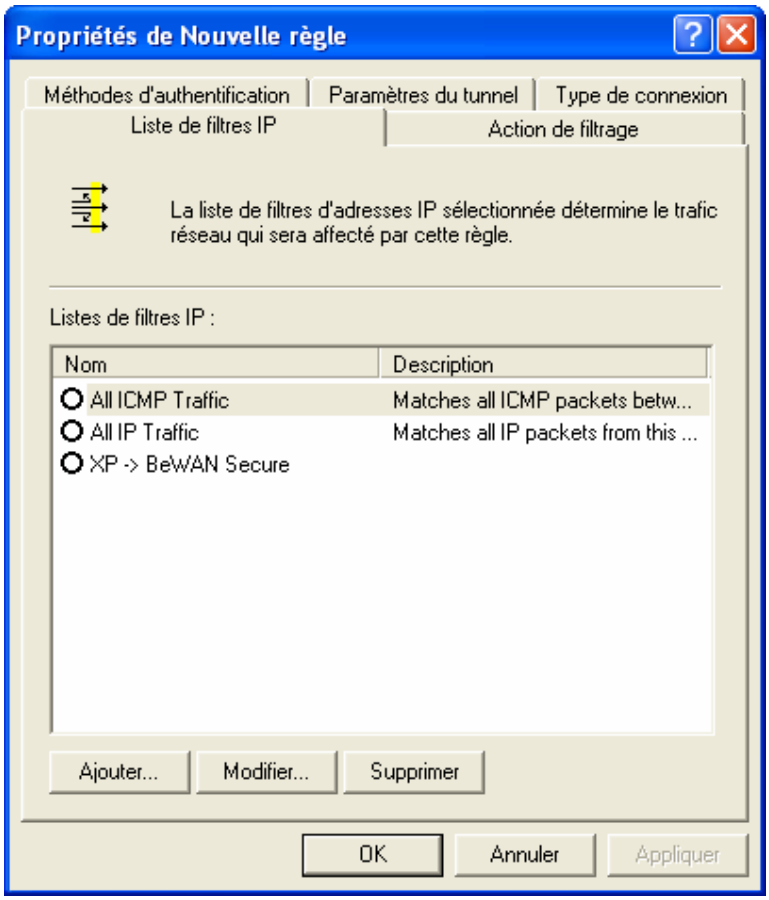
Cliquez sur **Appliquer**.


Propriétés de Nouvelle règle
Liste de filtres IP
Action de filtrage
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Le point d'arrêt du tunnel est l'ordinateur de tunneling le plus proche de la destination du trafic IP, tel que spécifié par la liste de filtres IP associés. Deux règles sont nécessaires pour décrire un tunnel IPSec.
Cette règle ne spécifie aucun tunnel IPSec.
Le point d'arrêt du tunnel est spécifié par cette adresse IP :
192 . 168 . 2 . 1
Fermer
Annuler
Appliquer

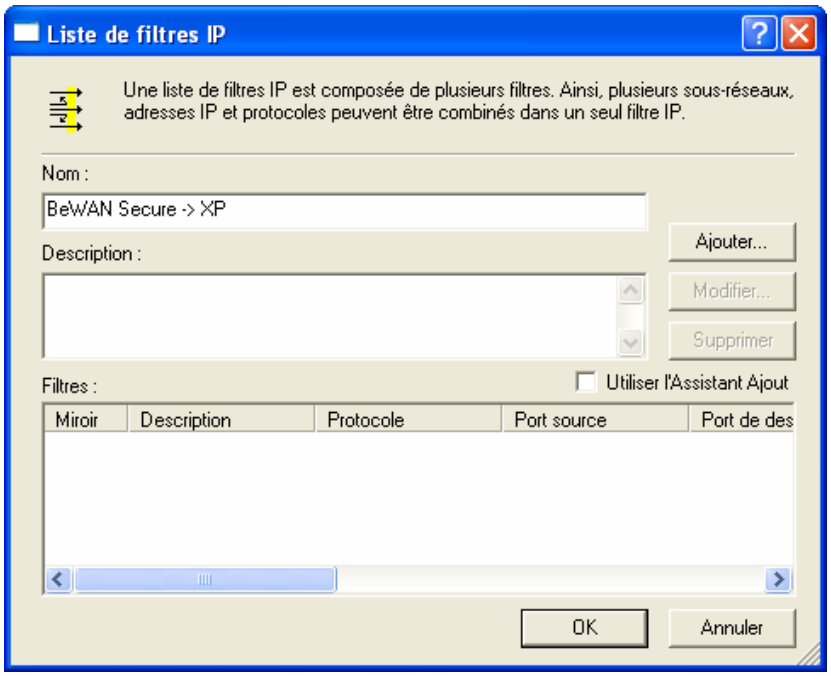
Sélectionnez la règle de sécurité IP ***XP -> BeWAN Secure*** prédéfinie. Cliquez sur **Ajouter…**.



Cliquez sur **Ajouter…**.



Entrez le nom de la liste de filtres IP inverse, ***BeWAN Secure -> XP***. Cliquez sur **Ajouter…**.

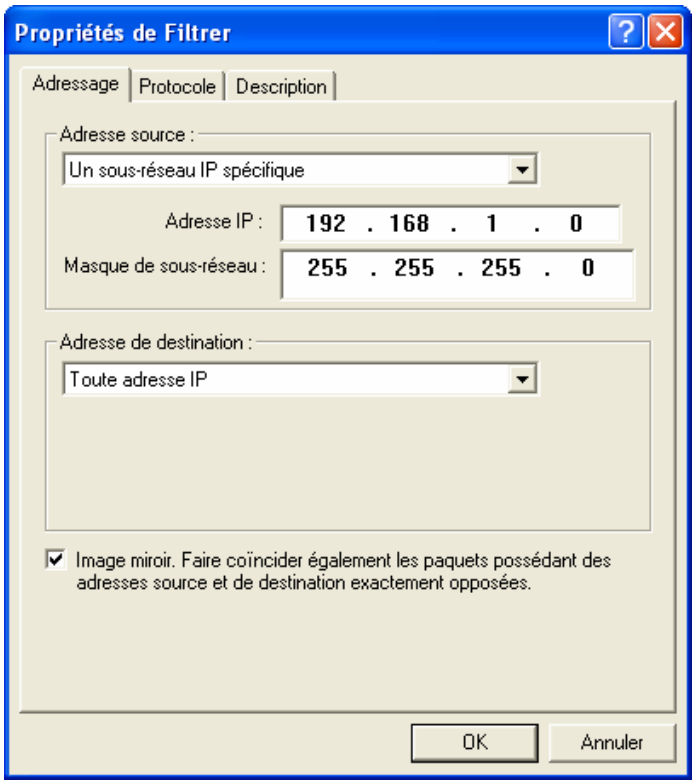


Sélectionnez **Un sous-réseau IP spécifique** dans la liste déroulante **Adresse source** et entrez le sous-réseau de l'extrémité opposée du tunnel VPN dans les champs **Adresse IP** et **Masque de sous-réseau** (192.168.1.0/255.255. 255.0). Sélectionnez la règle de sécurité IP ***XP -> BeWAN Secure*** prédéfinie.

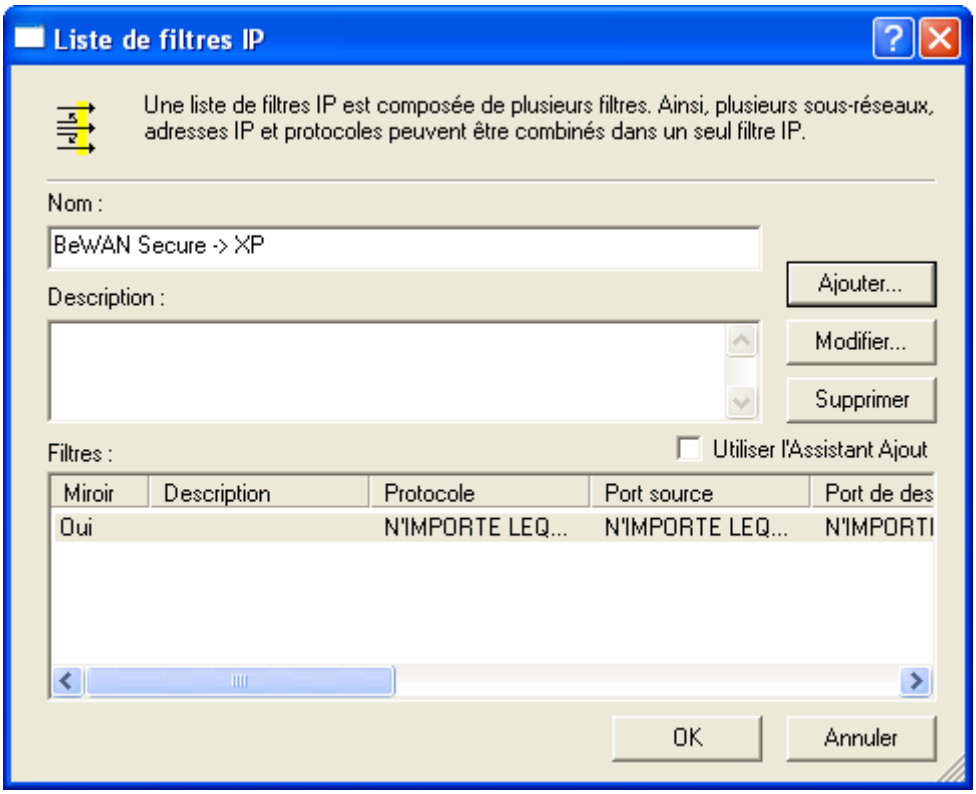
Dans la liste déroulante **Adresse de destination**, sélectionnez **Toute adresse IP**.

Cochez la case Image miroir. Faire coïncider également les paquets possédant des adresses source et de destination exactement opposées.

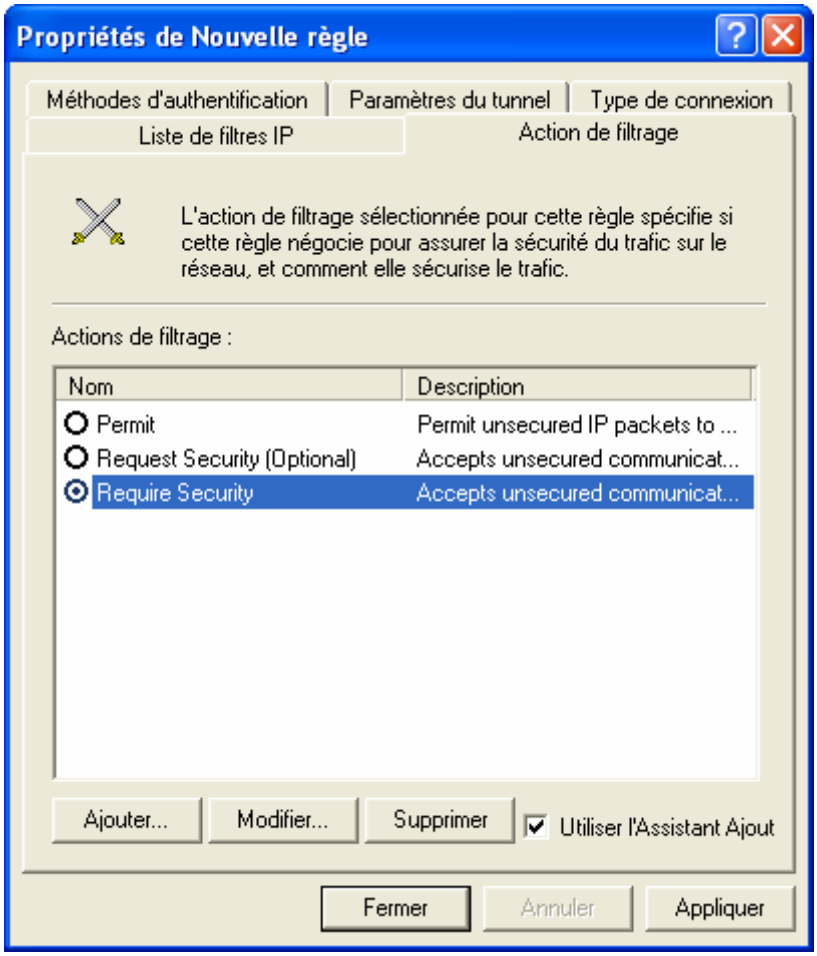
Cliquez sur **OK**.



Cliquez sur **OK**.



Sélectionnez **Require Security**. Cliquez sur **Modifier….**

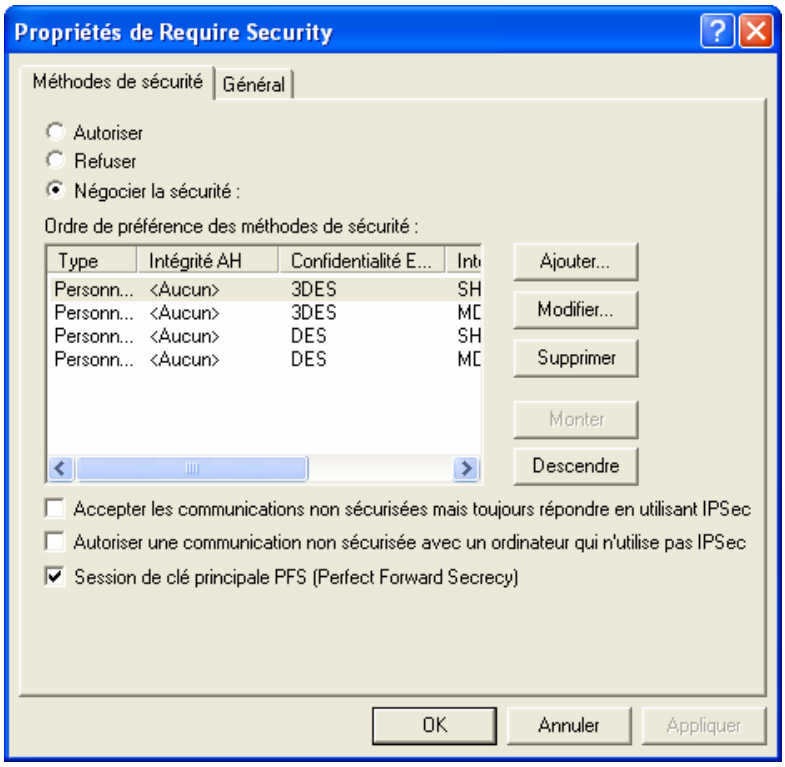


Sélectionnez Négocier la sécurité.

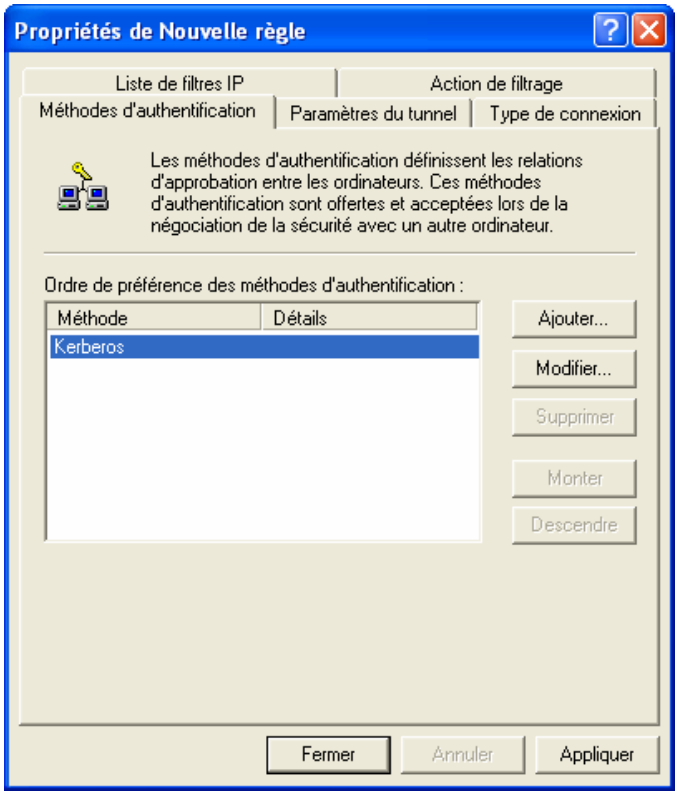
Vérifiez que les méthodes 3DES/SHA1 et 3DES/MD5 sont prises en charge.

Décochez la case Accepter les communications non sécurisées mais toujours répondre en utilisant IPSec. Cochez la case Session de clé principale PFS (Perfect Forward Secrecy).

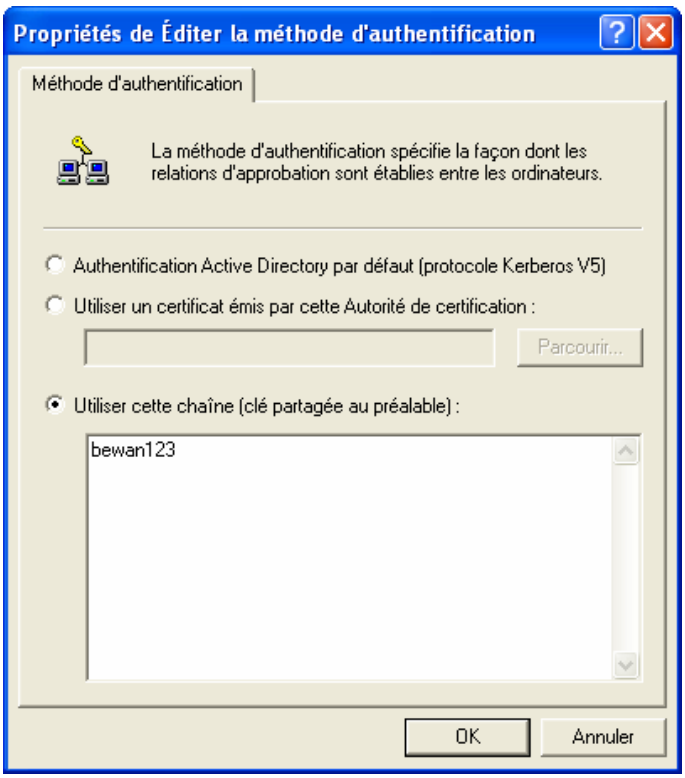
Cliquez sur **OK**.



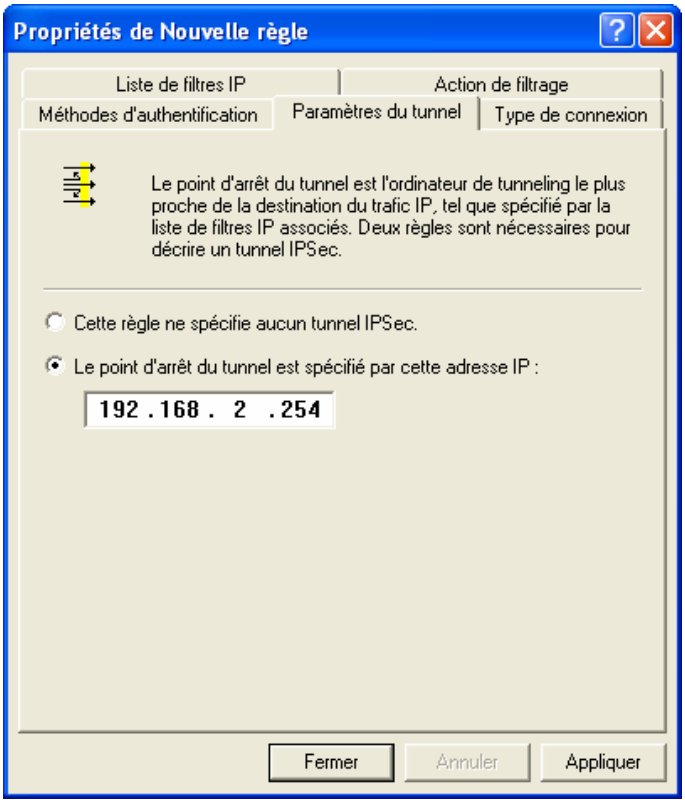
Cliquez sur **Modifier…**.



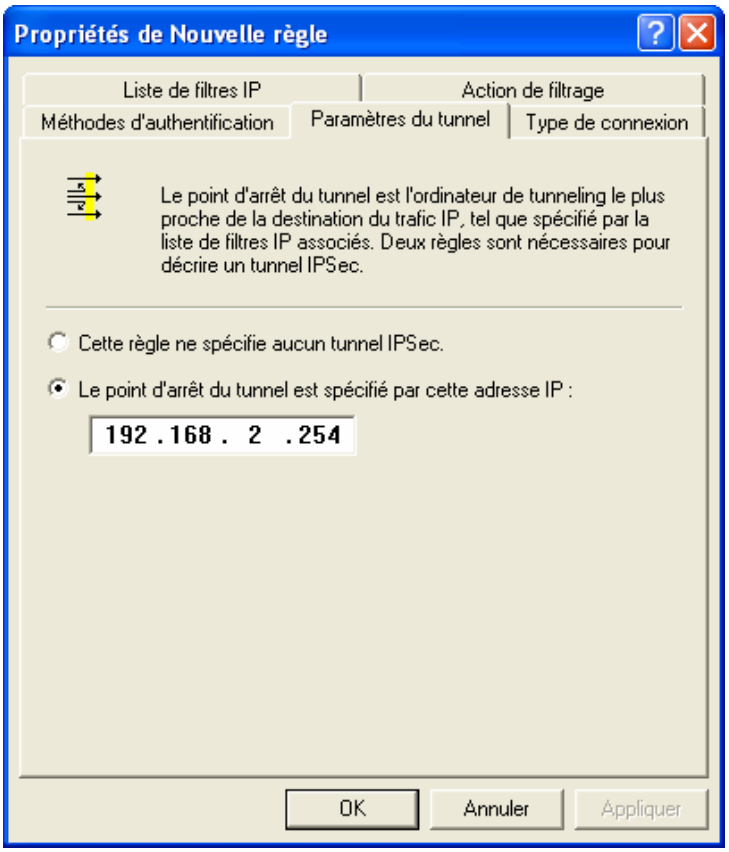
Sélectionnez Utiliser cette chaîne (clé partagée au préalable). Saisissez la clé prédéfinie : *bewan123*.
Cliquez sur **OK**.


Propriétés de Éditer la méthode d'authentification
Méthode d'authentification
La méthode d'authentification spécifie la façon dont les relations d'approbation sont établies entre les ordinateurs.
Authentification Active Directory par défaut (protocole Kerberos V5)
Utiliser un certificat émis par cette Autorité de certification :
Parcourir...
Utiliser cette chaîne (clé partagée au préalable) :
bewan123
OK
Annuler

Sélectionnez **Le point d'arrêt du tunnel est spécifié par cette adresse IP**.
Entrez l'adresse IP de l'interface WAN de l'hôte Windows XP (192.168.2.254 dans notre cas).
Cliquez sur **Appliquer**.

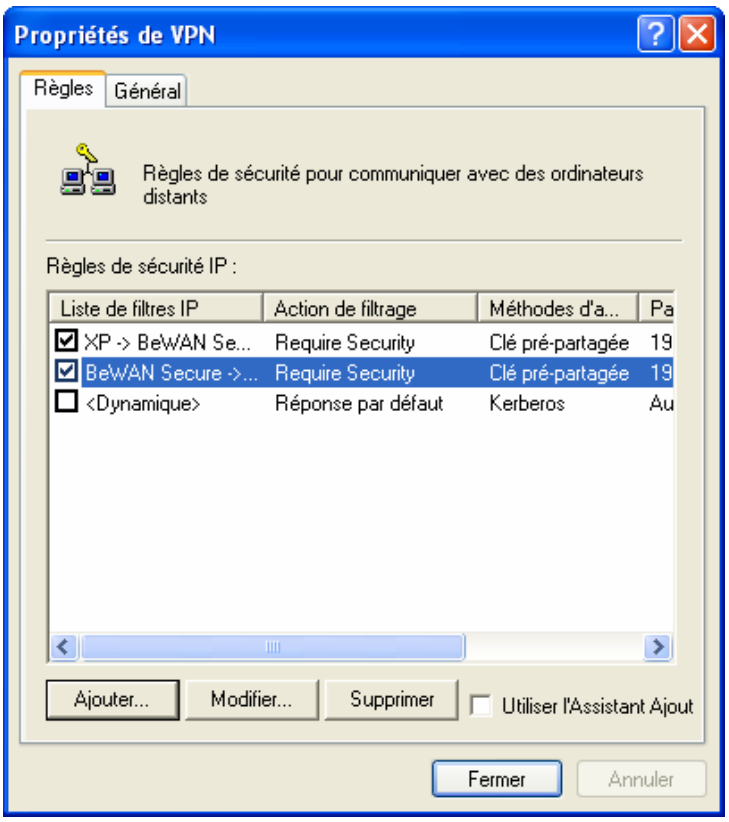

Propriétés de Nouvelle règle
Liste de filtres IP
Action de filtrage
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Le point d'arrêt du tunnel est l'ordinateur de tunneling le plus proche de la destination du trafic IP, tel que spécifié par la liste de filtres IP associés. Deux règles sont nécessaires pour décrire un tunnel IPSec.
Cette règle ne spécifie aucun tunnel IPSec.
Le point d'arrêt du tunnel est spécifié par cette adresse IP :
192 . 168 . 2 . 254
Fermer
Annuler
Appliquer

Cliquez sur **OK**.

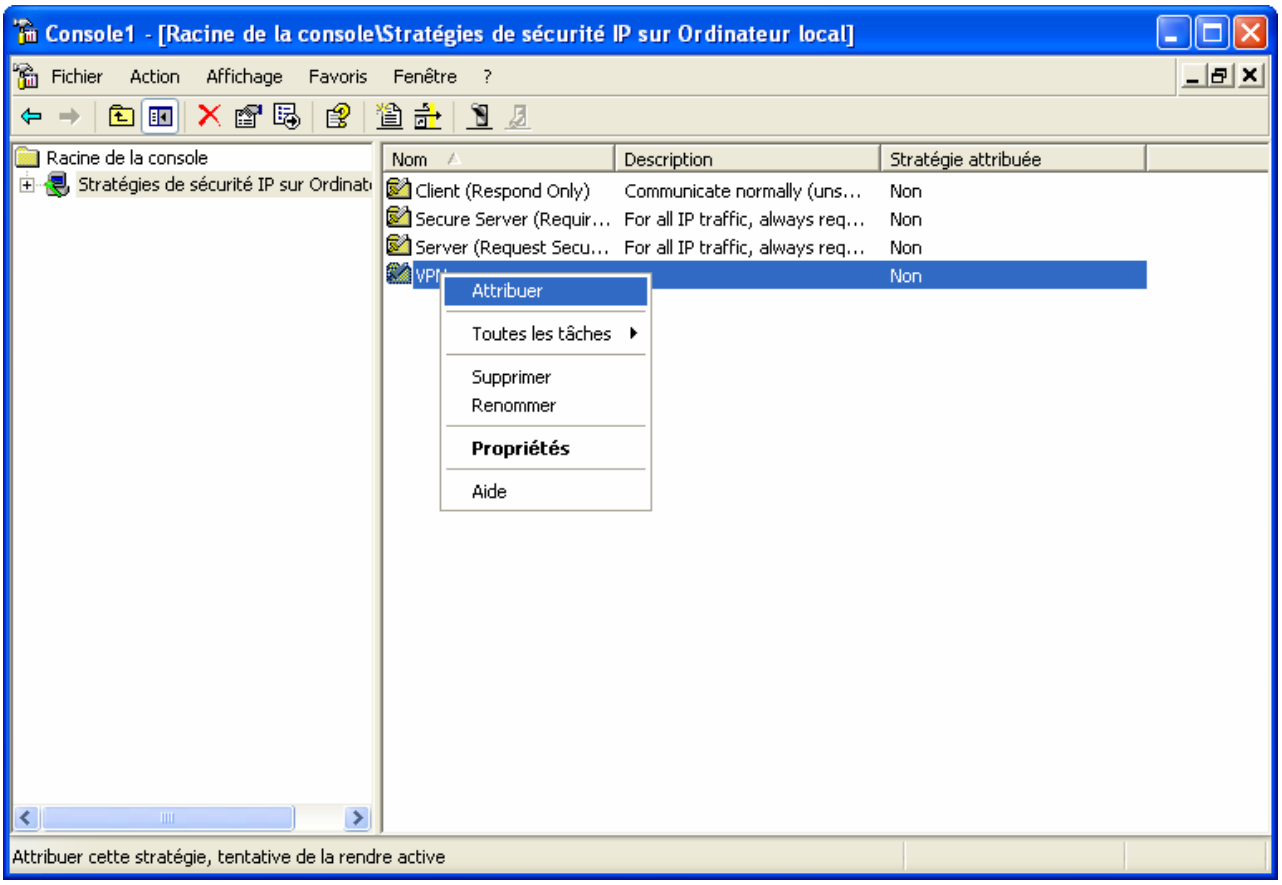

Propriétés de Nouvelle règle
Liste de filtres IP
Action de filtrage
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Le point d'arrêt du tunnel est l'ordinateur de tunneling le plus proche de la destination du trafic IP, tel que spécifié par la liste de filtres IP associés. Deux règles sont nécessaires pour décrire un tunnel IPSec.
Cette règle ne spécifie aucun tunnel IPSec.
Le point d'arrêt du tunnel est spécifié par cette adresse IP :
192 . 168 . 2 . 254
OK
Annuler
Appliquer

Veillez à cocher les deux règles de sécurité IP précédemment définies : ***XP -> BeWAN Secure*** et ***BeWAN Secure -> XP***.

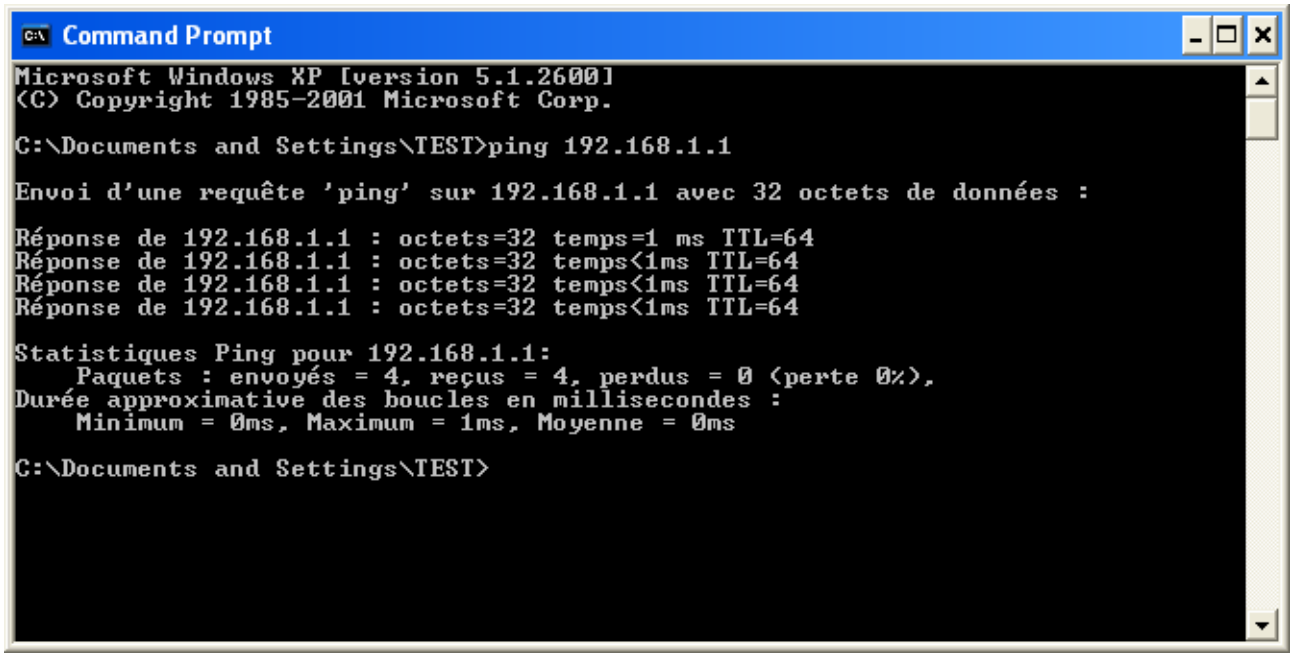
Cliquez sur **Fermer**.



Cliquez avec le bouton droit de la souris sur la stratégie de sécurité IP que vous venez de définir (***VPN*** dans notre cas). Cliquez sur **Attribuer**.



Lorsque vous cliquez sur la commande **Attribuer** du menu contextuel, l'hôte Windows XP établit un tunnel de réseau privé virtuel avec le routeur. Si le tunnel est correctement établi, l'écran suivant s'affiche durant l'exécution de l'outil Ping MS-DOS :


Command Prompt
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\TEST>ping 192.168.1.1
Envoi d'une requête 'ping' sur 192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64
Statistiques Ping pour 192.168.1.1:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
C:\Documents and Settings\TEST>

Vous pouvez afficher les informations du tunnel privé virtuel en sélectionnant **Réglages avancés > VPN > État IPSec VPN** dans l'administration Web du routeur.

SIP

Le serveur proxy SIP (***S**ession **I**nitiation **P**rotocol*, RFC 3261) peut traiter les paquets émis par les clients SIP (ayant l'adresse IP privée) pour qu'ils puissent franchir le pare-feu et la fonction NAT en réécrivant les informations SIP. Ainsi, le proxy SIP permet aux clients ayant l'adresse IP privée et tentant d'utiliser la téléphonie Internet, telle que Skype ou YamGTD, de franchir le pare-feu et la fonction NAT pour pouvoir communiquer avec leurs amis à l'aide d'un téléphone VoIP.

Le protocole SIP est défini pour autoriser les communications VoIP. En général, si votre routeur est doté d'un pare-feu ou d'une fonction NAT, les connexions VoIP sont refusées. Dans ce cas, le proxy SIP doit être activé pour que la fonction VoIP soit opérationnelle. Cliquez sur **Appliquer** pour que les modifications soient prises en compte.

État du serveur proxy SIP

Activer : active le serveur proxy SIP.

Désactiver : désactive le serveur proxy SIP.

Port d'écoute SIP

Paramètre par défaut : 5060 (doit être compris entre 1024 et 65536).

Port d'écoute RTP

Paramètre par défaut : 7070~7079 (doit être compris entre 1024 et 65536).

Routes statiques

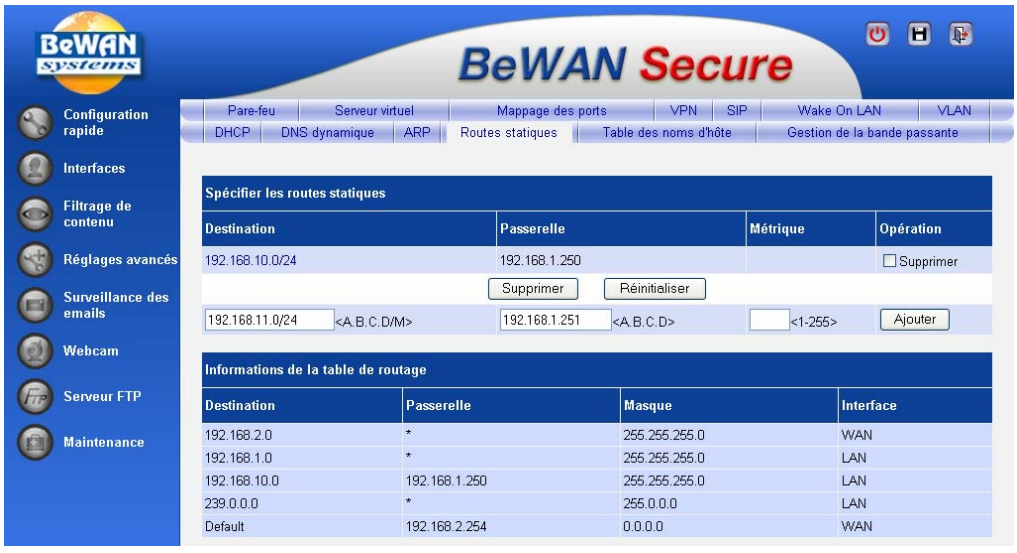
Si votre réseau local est constitué de plusieurs sous-réseaux, en plus du sous-réseau directement connecté au routeur, des routes statiques doivent être configurées vers les autres sous-réseaux (qui ne sont pas directement connectés au routeur). La page **Spécifier les routes statiques** comporte quatre sections : **Spécifier les routes statiques**, **Informations de la table de routage**, **Table ARP (table de traduction d'adresses MAC)** et **Table des noms d'hôte**.

SPECIFIER LES ROUTES STATIQUES

Supposons qu'il y ait trois sous-réseaux : 192.168.1.0/24, 192.168.10.0/24 et 192.168.11.0/24. La Passerelle A (192.168.1.250/24) est la passerelle entre les sous-réseaux 192.168.1.0/24 et 192.168.10.0/24. La Passerelle B (192.168.1.251/24) est la passerelle entre les sous-réseaux 192.168.1.0/24 et 192.168.11.0/24. En plus du paramétrage de l'adresse IP de l'interface LAN en tant que Passerelle A et Passerelle B, vous pouvez définir des routes statiques vers les sous-réseaux 192.168.10.0/24 et 192.168.11.0/24.

Sélectionnez **Routes statiques** dans le menu principal pour ouvrir la page de configuration. Remplissez les champs comme indiqué sur la capture d'écran ci-dessous. Cliquez sur **Ajouter**.

Dans l'illustration ci-dessous, la route statique pour le sous-réseau 192.168.10.0/24 est configurée. Veuillez ajouter une autre route statique.



Le système indiquera que deux routes statiques sont configurées.

Le paramètre **Métrique** n'est requis que si vous configurez plusieurs routes vers le même sous-réseau. Dans ce cas, le système prend la route dont la distance est la plus courte.

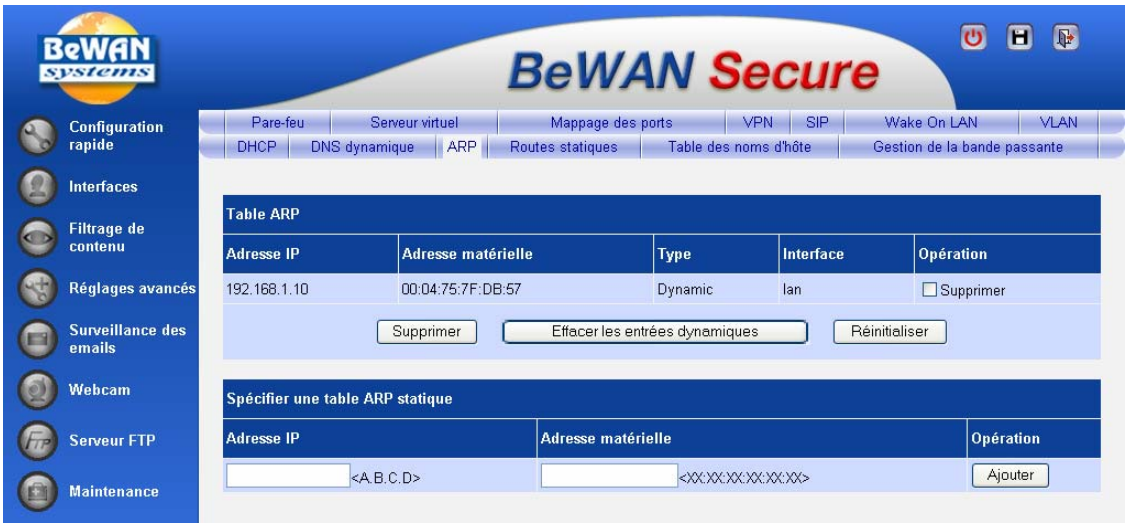
Pour supprimer une route statique, cochez la case **Supprimer** correspondante et cliquez sur le bouton **Supprimer**. Cliquez sur **Réinitialiser** pour annuler la sélection.

INFORMATIONS DE LA TABLE DE ROUTAGE

Les informations de la table de routage sont disponibles sur la page Routes statiques.

Table de traduction d'adresses MAC (Table ARP)

Avant la transmission des paquets, l'adresse MAC de l'hôte de destination doit être identifiée. Le routeur peut retenir automatiquement l'adresse MAC correspondant à une adresse IP. L'illustration ci-dessous présente la table de traduction.



La partie supérieure contient l'adresse MAC enregistrée automatiquement par le routeur. Le bouton **Effacer les entrées dynamiques** ne disparaît qu'après l'actualisation du système après une période de temps prédéfinie.

La colonne **Type** peut contenir deux valeurs : **Dynamic** et **Permanent**. Le type **Dynamic** indique que l'adresse MAC de l'hôte a été enregistrée automatiquement par le routeur. Le type Permanent indique qu'elle a été ajoutée manuellement.

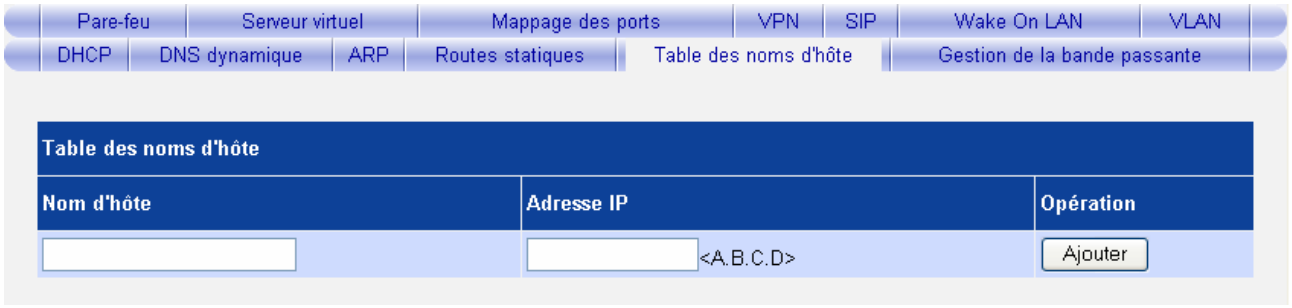
Pour supprimer une entrée de traduction d'adresse MAC, cochez la case correspondante et cliquez sur **Supprimer**. Cliquez sur **Réinitialiser** pour annuler l'action. Cliquez sur **Effacer les entrées dynamiques** pour effacer toutes les entrées enregistrées automatiquement dans la table. Pour les adresses MAC supprimées, l'adresse matérielle disparaît après son expiration. (« Incomplete » s'affiche si elle n'est pas encore expirée.)

La partie inférieure de la page permet de configurer manuellement la traduction d'adresses MAC. Entrez l'adresse IP de l'hôte dans le champ **Adresse IP** et l'adresse MAC dans le champ **Adresse matérielle**. Cliquez sur **Ajouter** pour que l'entrée soit prise en compte.

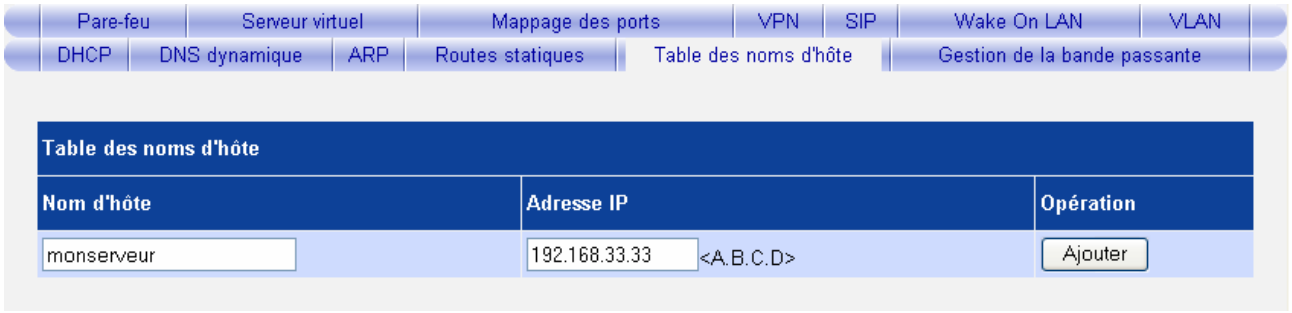
L'entrée de traduction d'adresse MAC configurée manuellement apparaîtra dans la partie supérieure de la page. Elle figure également dans la section **Spécifier une table ARP statique**. Pour supprimer une entrée de traduction ajoutée manuellement, utilisez la fonction de suppression de la section **Spécifier une table ARP statique**.

Table des noms d'hôte

Cette table met en correspondance les noms d'hôte et leur adresse IP. Elle est vide par défaut, comme représenté ci-dessous.



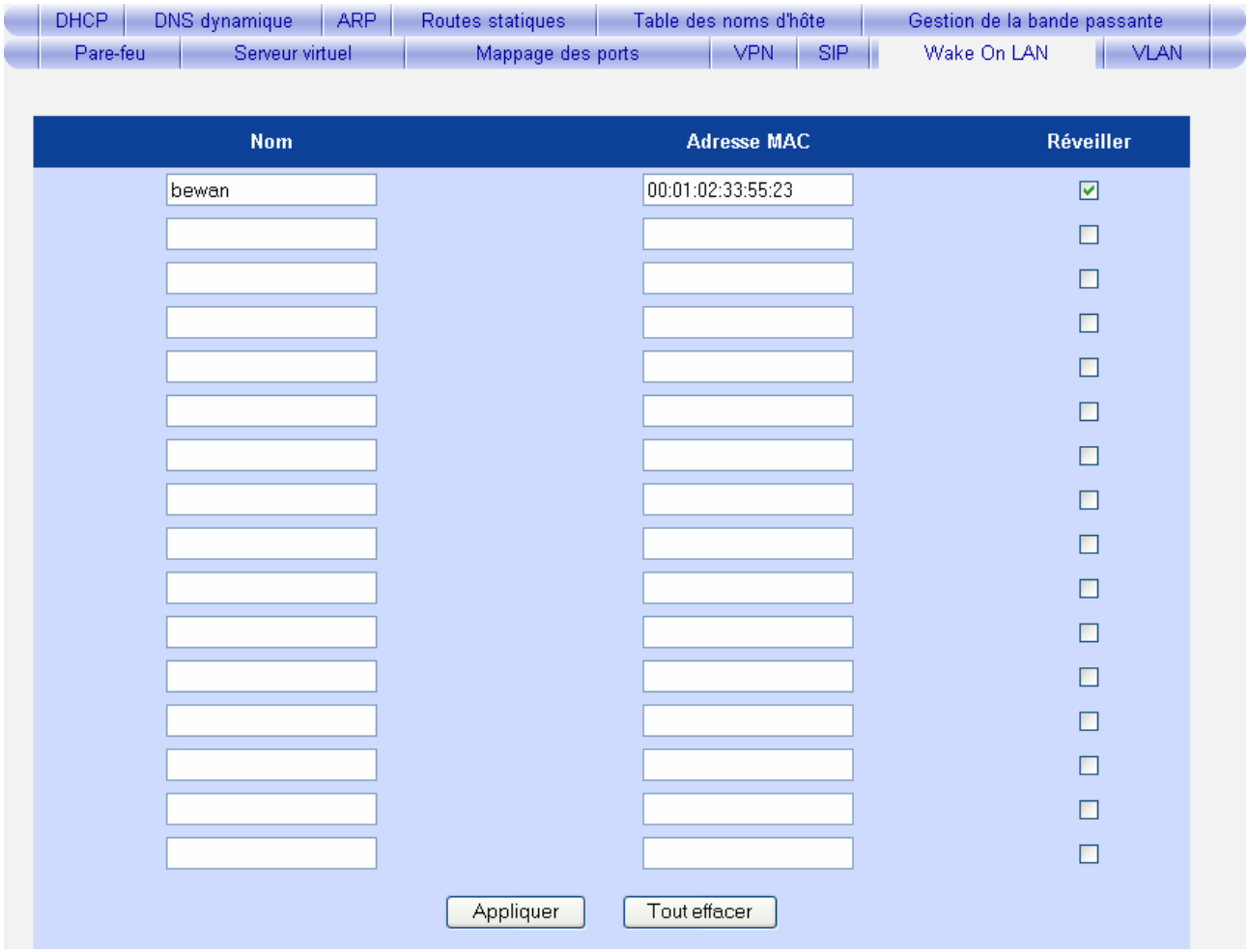
Si vous accédez régulièrement à l'hôte **monserveur** dont l'adresse IP est **192.168.33.33** et que le serveur DNS a des difficultés à établir la correspondance, vous pouvez l'ajouter à la table. Cliquez sur **Ajouter** pour que la correspondance soit prise en compte.



La table mise à jour est représentée ci-dessous. Pour supprimer une correspondance, cochez la case **Supprimer** et cliquez sur le bouton **Supprimer**. Cliquez sur **Réinitialiser** pour annuler l'action.

Wake On LAN

La fonction **Wake On LAN** permet de mettre un PC sous tension à distance. Pour utiliser cette fonction, vous devez l'activer dans le BIOS de l'ordinateur et disposer d'une carte réseau dotée d'une puce la prenant en charge. Reportez-vous à l'illustration ci-dessous pour configurer la mise sous tension à distance d'un PC.



Pour pouvoir mettre le PC sous tension à distance, vous devez saisir son **Adresse MAC**. Cochez la case **Réveiller**, puis cliquez sur le bouton **Appliquer** pour activer la fonction.

VLAN

Un VLAN (***V**irtuel **L**ocal **A**rea **N**etwork*) est une option de gestion de réseau permettant de répartir et d'organiser les éléments du réseau par regroupement logique des utilisateurs. Sur les BeWAN Secure série 50, la méthode de construction du VLAN s'effectue par port. Un VLAN est obtenu en associant chaque port à un VLAN.

L'administrateur peut ainsi parfaire les performances de communication et optimiser l'utilisation des ressources. Les avantages du VLAN peuvent être les suivants :

- la réduction de la diffusion du trafic. En créant des VLAN ou des groupes d'utilisateurs destinés à ne travailler qu'entre eux sur le réseau local, vous contrôlez les échanges entre les différents LAN, les messages de diffusion étant limités à l'intérieur de chaque VLAN.
- une meilleure utilisation de la bande passante.
- l'amélioration de la sécurité.

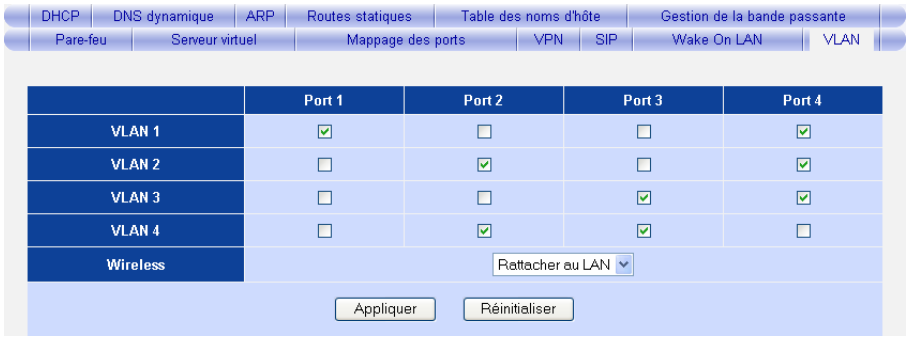
Pour configurer le VLAN, vous pouvez suivre l'exemple suivant.

Vous pouvez créer 4 VLAN au maximum qui seront constitués par groupes d'utilisateurs et favoriser ou non l'un d'entre eux.

Dans une société, considérons que nous regroupons :

- le service Comptabilité sur le port 1,
- le service Commercial sur le port 2,
- le service Marketing sur le port 3,
- un serveur de fichiers et de messagerie sur le port 4, où chaque utilisateur possède un répertoire propre avec ses dossiers courants.

Créez les VLAN suivants : un VLAN associant le port 1 et le port 4, un autre les ports 2 et 4, un troisième les ports 3 et 4, et enfin un dernier réunissant les ports 2 et 3.



Vous autorisez donc la communication entre chaque service et le port 4 qui est constitué des serveurs. Vous autorisez également la diffusion d'informations entre le service Marketing et le service Commercial. En groupant plusieurs ports dans un VLAN, vous permettez ainsi à des paquets d'être envoyés aux ports constituant le même VLAN sans générer de trafic sur les autres ports.

De ce fait, le communication par exemple entre les postes du service Comptabilité (port 1) et du service Marketing (port 3) sera impossible.

N'importe quel port peut faire partie d'un VLAN et un port peut appartenir à des VLAN différents. En configurant vos ports par VLAN, vous améliorez l'utilisation des ressources du réseau et la sécurité du réseau.

Surveillance des emails

La Surveillance des emails permet de surveiller les e-mails entrants. Vous pouvez prédéfinir les groupes de mails et les serveurs de mails de certains correspondants. Lorsque ces derniers vous enverront un e-mail, le voyant E-mail situé en face avant de l'appareil clignotera en fonction de votre paramétrage.

Cette page est composée de deux sections : Groupes de mail et Serveurs de mails. Elles peuvent être configurées dans n'importe quel ordre.

Groupes de mail

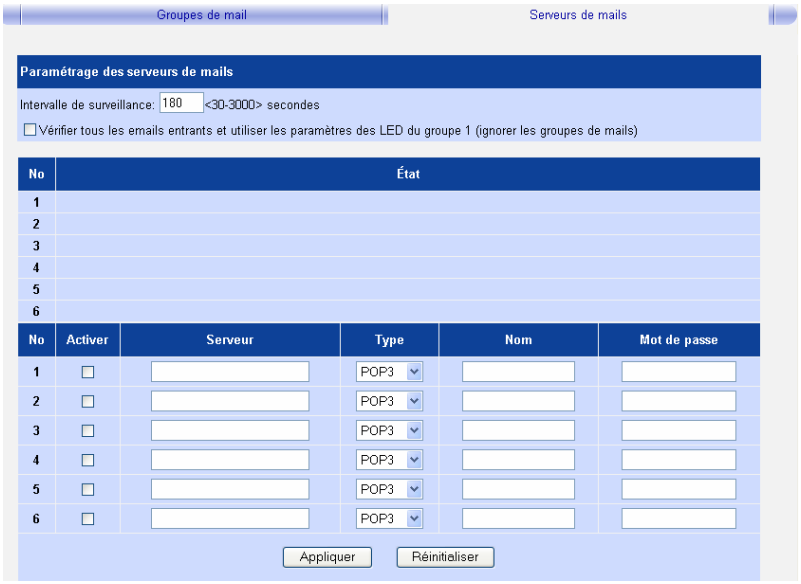
Vous pouvez définir jusqu'à six groupes de courrier entrant. Les chaînes définissant les groupes peuvent comporter jusqu'à six caractères. Si l'adresse e-mail de l'expéditeur contient la chaîne définie pour un groupe, le système considère que l'expéditeur appartient à ce groupe et fait clignoter le voyant E-mail en conséquence. Lorsqu'il y a plusieurs e-mails de groupes différents, le système les indique par ordre de priorité. (Le groupe 1 a la priorité la plus haute et le groupe 6, la plus basse.)

Groupes de mail
Serveurs de mails
Paramétrage des groupes de mails
Veuillez indiquer l'adresse email complète ou partielle.
Groupe 1 a la plus haute priorité pour l'affichage des LED.
Groupe 1
LED1: Clignote LED2: Clignote
No.1 Partial / Full Sender's E-Mail Address:
No.2 Partial / Full Sender's E-Mail Address:
No.3 Partial / Full Sender's E-Mail Address:
No.4 Partial / Full Sender's E-Mail Address:
No.5 Partial / Full Sender's E-Mail Address:
No.6 Partial / Full Sender's E-Mail Address:
Groupe 2
LED1: Allumée LED2: Allumée
No.1 Partial / Full Sender's E-Mail Address:
No.2 Partial / Full Sender's E-Mail Address:

La capture d'écran ci-dessus est légèrement différente de l'écran réel (les groupes 3 à 6 et une partie du groupe 2 ne sont pas représentés). Pour définir ou modifier une chaîne de reconnaissance d'e-mail, saisissez ou modifiez-la directement et cliquez sur le bouton **Appliquer**. Cliquez sur le bouton **Réinitialiser** pour annuler toutes les modifications.

Serveurs de mails

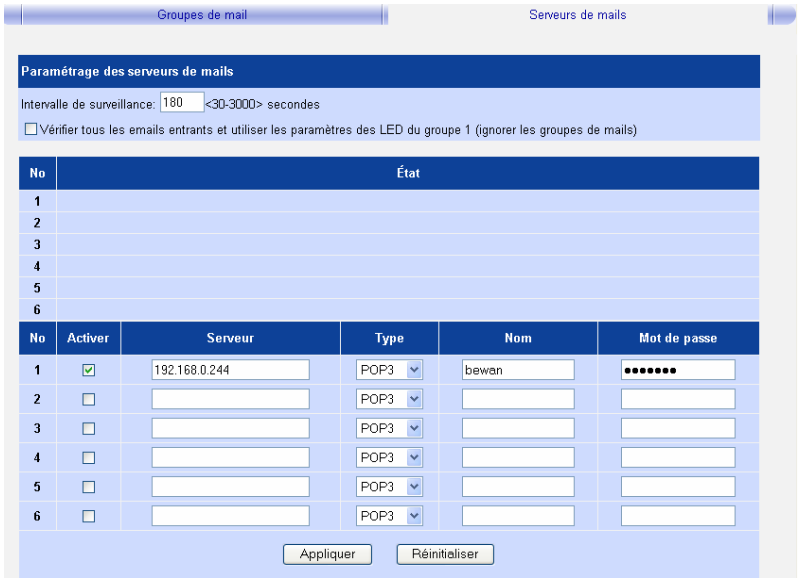
La capture d'écran ci-dessous représente la page de configuration **Serveurs de mails**.



L'intervalle de surveillance des nouveaux e-mails par défaut est de 3 minutes. Vous pouvez ignorer les groupes de mails pour l'alerte e-mail ; dans ce cas, les paramètres des voyants du premier groupe de mails seront utilisés. Si vous modifiez les informations des serveurs ou des groupes de mails, cliquez sur Appliquer pour confirmer les modifications.

Vous pouvez définir jusqu'à six serveurs de mails. La colonne **État** affiche l'état actuel de chaque serveur. Le tableau représenté ci-dessous permet de définir les serveurs de mails. Saisissez respectivement le nom du serveur, le type de connexion (POP3, POP3S, IMAP, IMAPS), le nom d'utilisateur et le mot de passe. Pour activer un serveur, cochez la case **Activer** correspondante. Cliquez sur **Appliquer** pour que les modifications soient prises en compte. Cliquez sur **Réinitialiser** pour annuler les modifications.

Pour activer un serveur, cochez la case **Activer** correspondante. Après avoir ajouté ou modifié un serveur, cliquez sur le bouton **Appliquer** pour activer la configuration. Cliquez sur le bouton **Réinitialiser** pour annuler les modifications.



Fonction Webcam

Les modèles BeWAN Secure M50 et M50G sont dotés d'un serveur de webcam intégré. En connectant une webcam au routeur, l'utilisateur peut surveiller son domicile ou son bureau à distance. Le routeur prend en charge la détection dynamique qui permet de détecter les activités ou mouvements suspects et d'envoyer une alerte e-mail contenant les images capturées à l'adresse e-mail indiquée (enregistrement numérique lorsqu'il est raccordé à une webcam compatible ; le système doit être connecté à un périphérique de stockage USB).

Attention : cette fonction n'est compatible qu'avec certains modèles de webcams. Veuillez vous reporter à l'annexe A pour connaître la liste de ces modèles.

Configuration de la webcam

La configuration de la webcam se décompose en trois parties : configuration de la détection de mouvement, paramétrage de la planification et paramétrage du mail. La Détection de la capture ne s'active que lorsque le **Serveur de webcam** est activé ; de même, l'Enregistrement ne s'active que lorsque la **Détection de la capture** est activée. Chacun des paramètres de configuration est décrit ci-dessous :

REGLAGE

Server de webcam

Les fonctions telles que **Détection de la capture**, **Enregistrement**, **Planification de détection** et **Alerte par Email** ne fonctionnent que lorsque le Serveur de webcam est activé.

Détection de la capture

Activez la fonction **Détection de la capture**. Après son activation, le système enverra un message d'alerte dès que le rapport de mouvement détecté dans l'environnement sera supérieur au Seuil défini.

Enregistrement

Si le système est connecté à un périphérique de stockage USB, vous pouvez activer la fonction d'enregistrement numérique. Si aucun répertoire ne porte le nom indiqué sur la partition sélectionnée au moment de l'activation, le système crée automatiquement ce répertoire. Une fois démarré, l'enregistrement numérique s'arrête automatiquement après 60 secondes d'inactivité (aucun mouvement détecté). Il redémarrera automatiquement par la suite si le pourcentage de différence des images excède le seuil défini. La vidéo est enregistrée au format Motion JPEG. Si vous la lisez sous Windows, DirectX 8.0 ou supérieur doit être installé.

Taille de l'image capturée

Sélectionnez la taille de l'image à capturer.

Seuil

Spécifiez le pourcentage de différence des images maximal acceptable. Lorsque le pourcentage de différence des images excède la valeur spécifiée, le système envoie des alertes par e-mail et lance immédiatement l'enregistrement numérique selon les configurations définies.

Niveau de bruit

Saisissez la valeur du niveau de bruit. Aucun mouvement n'est pris en compte sous le niveau de bruit. Par conséquent, plus cette valeur est basse, plus la fonction de détection de mouvement est sensible. Ignorez ce champ si cette dernière est désactivée.

Délai

Après l'activation de la détection de mouvement, le système retardera le lancement effectif de la détection pendant le nombre de secondes spécifié ici.

Email avec capture d'image

Sélectionnez **Non** pour que le message d'alerte envoyé par la détection de mouvement ne contienne que du texte. Sélectionnez **Oui** pour que le message contienne également les images capturées.

Nombre d'emails maximum pendant 1 minute

Saisissez le nombre maximum d'alertes par e-mail envoyées en une minute. Entrez 0 pour n'imposer aucune limite. La valeur par défaut est 5.

Cliquez sur **Appliquer** pour activer la fonction de détection de mouvement. Cliquez sur **Réinitialiser** pour annuler toutes les modifications.

PLANIFICATION DE DETECTION

Les fonctions relatives au système de détection de mouvement définies sur Activer peuvent être activées via un calendrier sur une base quotidienne ou hebdomadaire. Pour définir un calendrier, cliquez sur **Planification de détection** et entrez les horaires de début et de fin souhaités dans les champs prévus à cet effet.

Cliquez sur **Appliquer** quand vous avez terminé. Cliquez sur **Réinitialiser** pour annuler toutes les modifications.

ALERTE PAR EMAIL

Dans la section **Paramétrage du mail**, entrez les informations des serveurs de messagerie auxquels les alertes par e-mail doivent être envoyées lorsque le pourcentage de différence entre les images capturées excède le seuil défini. Vous devez fournir les renseignements suivants : **Serveur de mails**, **Adresse email**, **Nom d'utilisateur** et **Mot de passe**. Cliquez sur **Appliquer** lorsque vous avez terminé.

Cliquez sur **Appliquer** lorsque vous avez terminé pour que la modification soit prise en compte. Cliquez sur **Réinitialiser** pour annuler toutes les modifications.

Webcam en direct

Cliquez sur **Webcam en direct** dans le menu principal pour accéder à la fonction de surveillance en direct et à distance de l'environnement (voir la capture d'écran ci-dessous). Une seule webcam peut être connectée et utilisée à la fois.

Serveur FTP

Pour pouvoir accéder au serveur FTP ou le configurer, vous devez connecter le système à un périphérique de stockage USB :

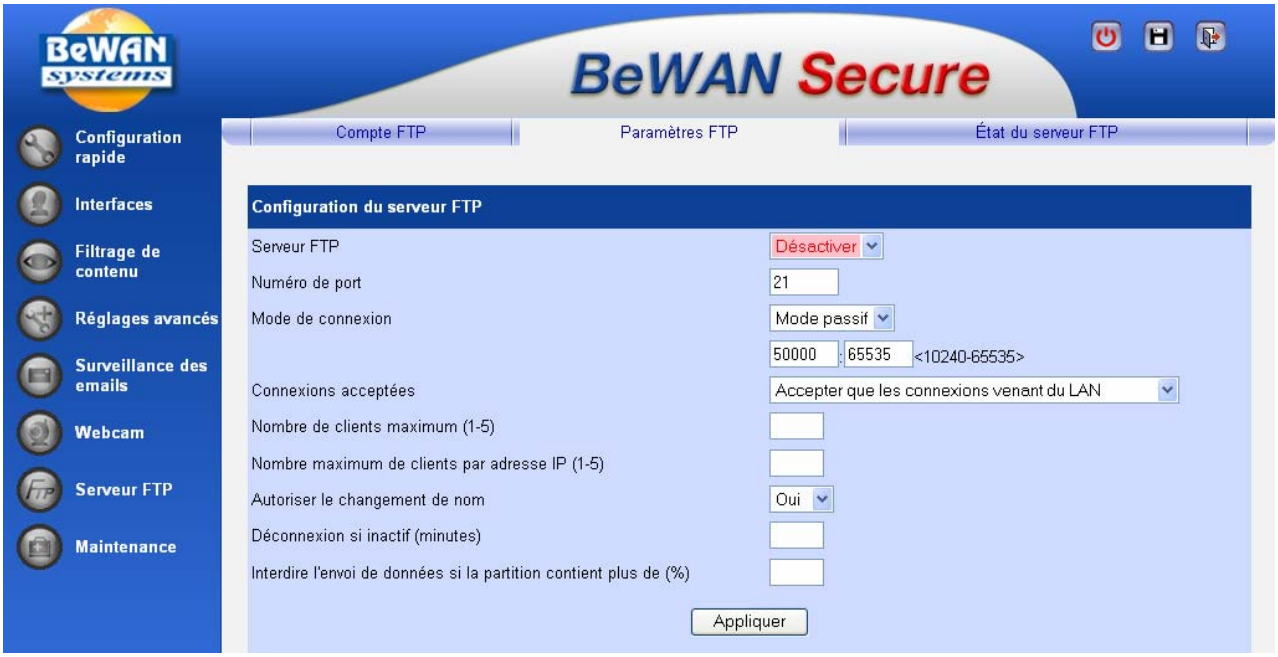
- disque dur USB (avec adaptateur secteur externe),
- clé USB,
- appareil photo numérique,
- lecteur MP3,
- lecteur de cartes USB.

En connectant l'un de ces périphériques, les utilisateurs peuvent facilement configurer un serveur FTP pour partager ou télécharger les fichiers d'utilisateurs locaux ou distants. Le serveur FTP intégré permet de définir plusieurs comptes FTP, le contrôle d'accès, le contrôle de la bande passante en émission/réception, le ratio réception/émission, l'adresse IP source, etc.

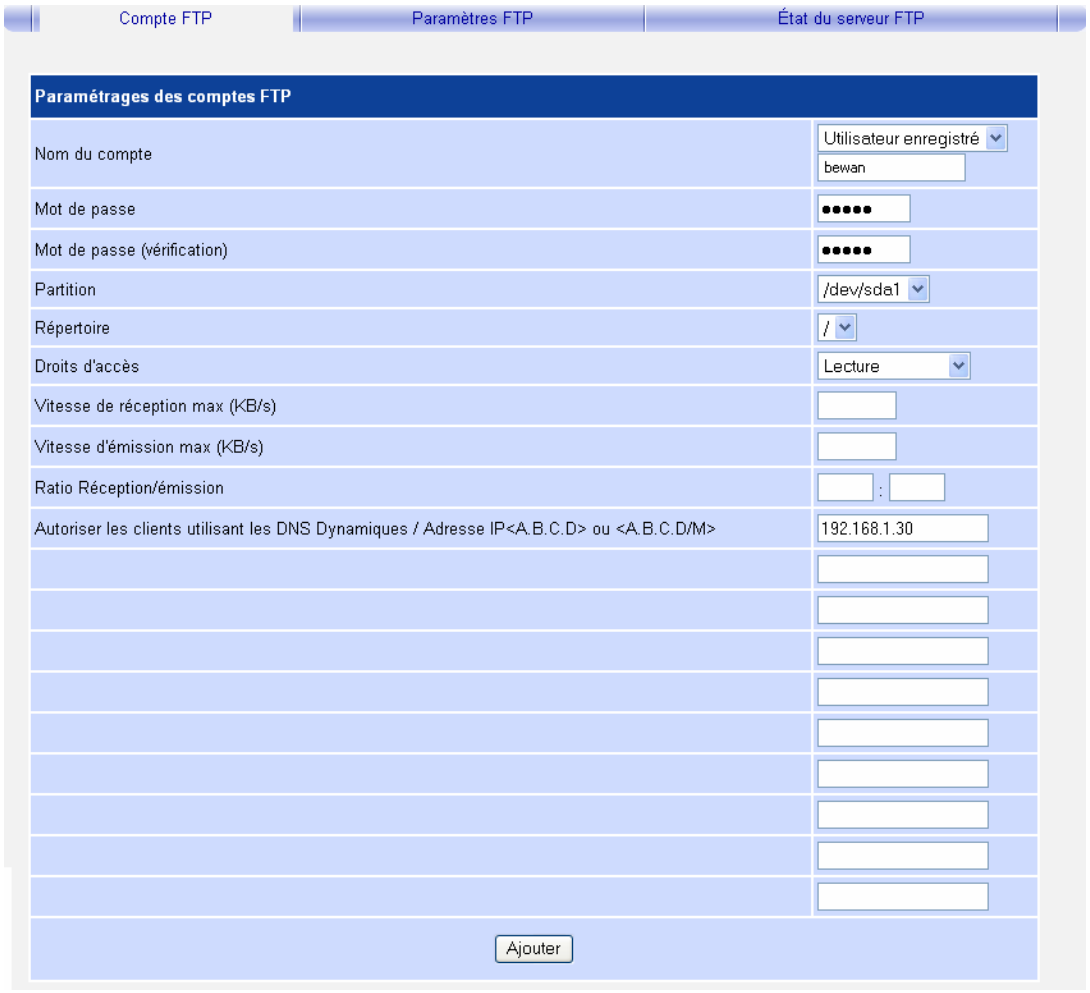
Attention : le serveur FTP est compatible avec les périphériques de stockage USB utilisant le format FAT32 ou EXT2. Si vous devez formater votre périphérique de stockage USB, veillez à utiliser le format FAT32 ou EXT2.

Paramètres FTP

Lorsque vous activez le serveur FTP, le routeur vérifie si un compte FTP a été créé. Par conséquent, vous devez créer un compte FTP avant d'activer le serveur FTP. Pour configurer ce dernier, cliquez sur **Serveur FTP** dans le menu principal, puis sur **Paramètres FTP**. Pour configurer un serveur FTP de base, suivez les instructions ci-dessous :



Compte FTP



Les paramètres de configuration du compte sont les suivants :

Nom du compte

Le nom du compte FTP. Si vous sélectionnez **Utilisateur enregistré**, saisissez le nom d'utilisateur ; si vous sélectionnez **Utilisateur anonyme**, le système définit le nom d'utilisateur sur anonyme.

Mot de passe

Le mot de passe de l'utilisateur. Il n'est pas nécessaire de définir un mot de passe pour l'**Utilisateur anonyme**.

Mot de passe (vérification)

Saisissez à nouveau le mot de passe pour que le système le compare à celui précédemment entré.

Partition

Indiquez la partition du disque sur laquelle se trouve le répertoire racine de l'utilisateur. Le système recherche automatiquement les partitions disponibles et vous les propose. Il prend en charge les systèmes de fichiers FAT32 et EXT2.

Répertoire

Le nom du répertoire racine de l'utilisateur.

Droits d'accès

Les droits d'accès de l'utilisateur : sélectionnez Lecture pour n'autoriser que la réception de données et Lecture/Écriture pour autoriser la réception et l'émission de données.

Vitesse de réception max (KB/s)

Limite la vitesse de réception de l'utilisateur (Kilo-octets/s).

Vitesse d'émission max (KB/s)

Limite la vitesse d'émission de l'utilisateur (Kilo-octets/s).

Ratio Réception/émission

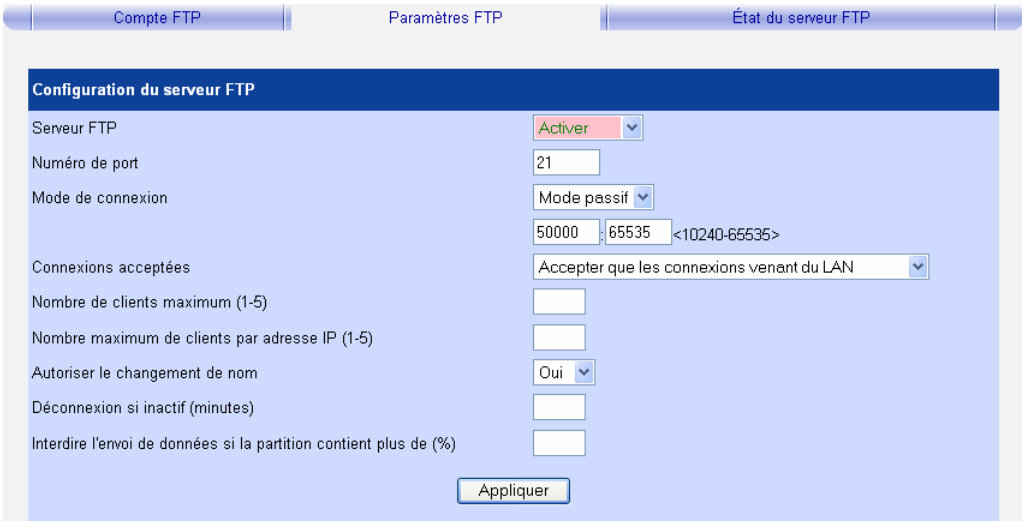
Configurez le ratio de données reçues/émises. Les utilisateurs ne peuvent recevoir aucune donnée si le ratio est inférieur à celui spécifié.

Autoriser les clients utilisant les DNS Dynamiques / Adresse IP<A.B.C.D> ou <A.B.C.D/M>

Indiquez depuis quelles adresses IP ou depuis quels domaines les clients peuvent se connecter à ce serveur FTP. Chaque compte peut contenir 10 groupes d'adresses ou de sous-réseaux source.

Créez un compte pour activer le serveur FTP. Si vous n'avez pas créé le répertoire privé de chaque utilisateur sur la partition de disque que vous souhaitez utiliser, vous pouvez définir un utilisateur ayant un accès en lecture/écriture sur cette partition et vous connecter au serveur avec ce compte pour créer les différents répertoires privés. Si vous souhaitez créer un utilisateur ayant le nom racine et limiter son accès à l'adresse 192.168.1.30, votre saisie doit correspondre à celle présentée plus haut.

Cliquez sur **Ajouter** après avoir fourni les informations ci-dessus. Vous pouvez ensuite activer le serveur.



Le compte .racine. que vous venez d'ajouter apparaît sous l'écran de configuration. Les paramètres du serveur FTP sont :

Serveur FTP

Sélectionnez **Activer** pour activer le serveur FTP, **Désactiver** pour le désactiver.

Numéro de port

Le numéro de port sur lequel écoute le serveur FTP. La valeur par défaut est 21.

Mode de connexion

Mode actif ou **Mode passif**. Le mode passif offre une plus grande compatibilité. Si le client est derrière un pare-feu ou une passerelle NAT, il est recommandé d'utiliser le mode passif.

Connexions acceptées

Les adresses IP des interfaces WAN et LAN du routeur peuvent être utilisées pour identifier le serveur FTP. Sélectionnez **Accepter que les connexions venant du LAN** pour activer le serveur FTP dans le réseau local. Sélectionnez **Accepter les connexions venant du LAN et du WAN** pour activer le serveur FTP pour les utilisateurs distants.

Nombre de clients maximum (1-5)

Le nombre maximum de clients que le système accepte. La valeur par défaut est 5.

Nombre maximum de clients par adresse IP (1-5)

Le nombre maximum de clients pouvant se connecter par adresse IP. Le nombre total de clients pouvant se connecter depuis la même adresse IP est limité par cette valeur.

Autoriser le changement de nom

Si vous sélectionnez **Oui**, les fichiers peuvent être renommés.

Déconnexion si inactif (minutes)

Si l'utilisateur n'effectue aucune action pendant cette durée, le système le déconnecte automatiquement. La valeur par défaut est 15 minutes.

Interdire l'envoi de données si la partition contient plus de (%)

Si la quantité d'espace de stockage occupée est supérieure à cette valeur, le système interdit l'envoi de données.

Cliquez sur **Appliquer** après avoir fourni les informations ci-dessus. Activez le serveur FTP.

Connexion au serveur FTP depuis Windows

Après avoir effectué la configuration comme décrit plus haut, vous pouvez accéder au serveur FTP sous Windows via une page Web en saisissant son adresse IP unique. Le format de l'adresse IP FTP est le suivant :

ftp://Nom-du-compte@Adresse IP WAN (le mot de passe doit être saisi à la connexion)

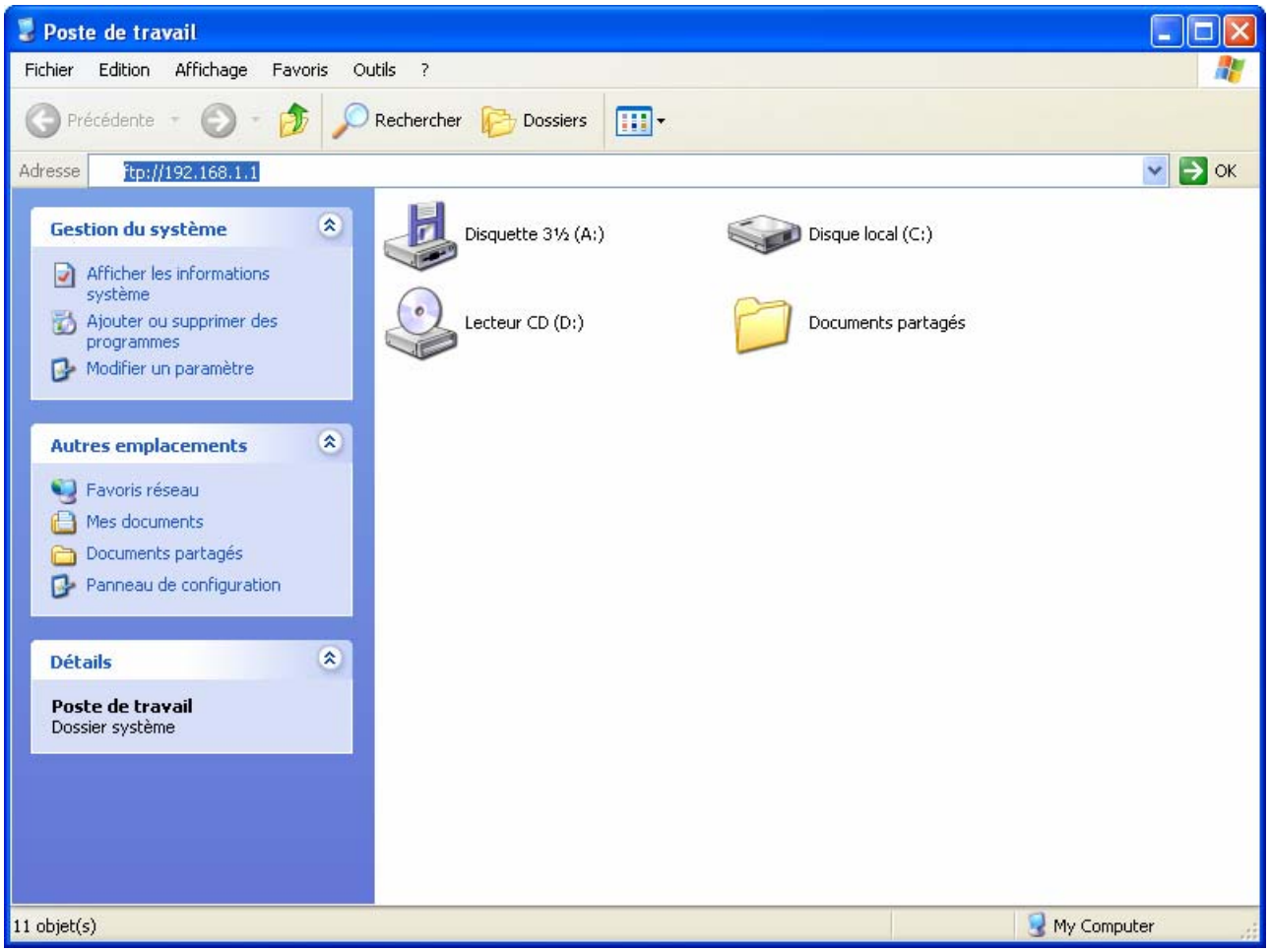
ftp://Nom-du-compte:Mot-de-passe@Adresse IP WAN (inutile de saisir le mot de passe à la connexion)

UTILISATION DE WINDOWS XP

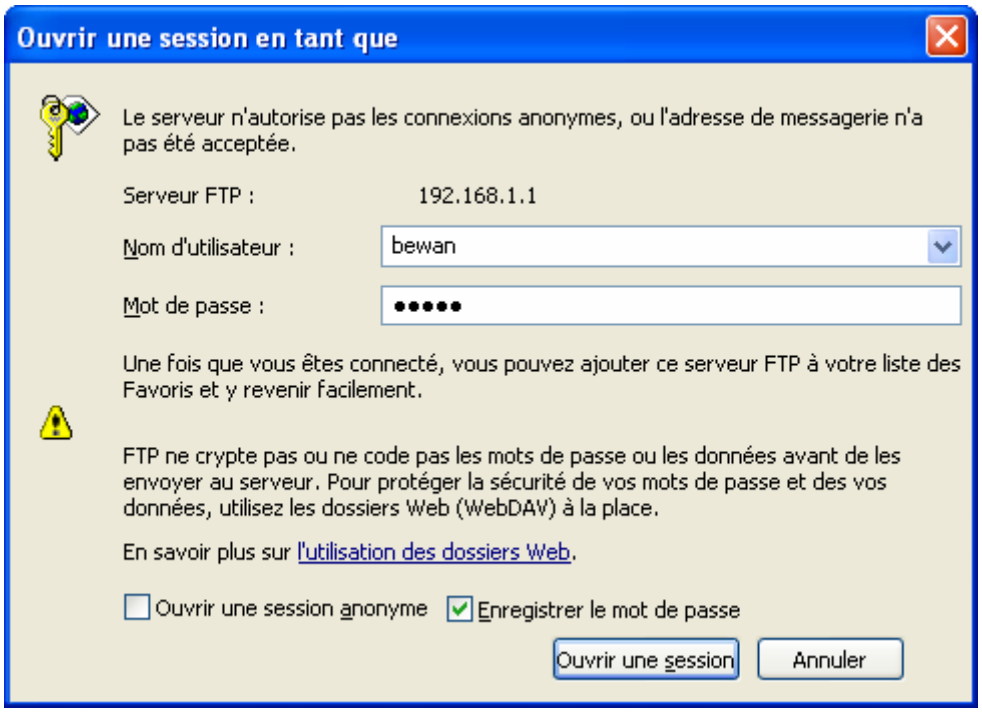
En reprenant l'exemple ci-dessus, si vous utilisez Windows XP, le nom de compte du serveur FTP que vous avez configuré est .racine., l'adresse IP de votre interface LAN est ***192.168.1.1*** et le mot de passe est ***bewan***. Votre adresse IP FTP devrait être :

ftp://bewan@192.168.1.1 ou ftp://bewan:bewan@192.168.1.1

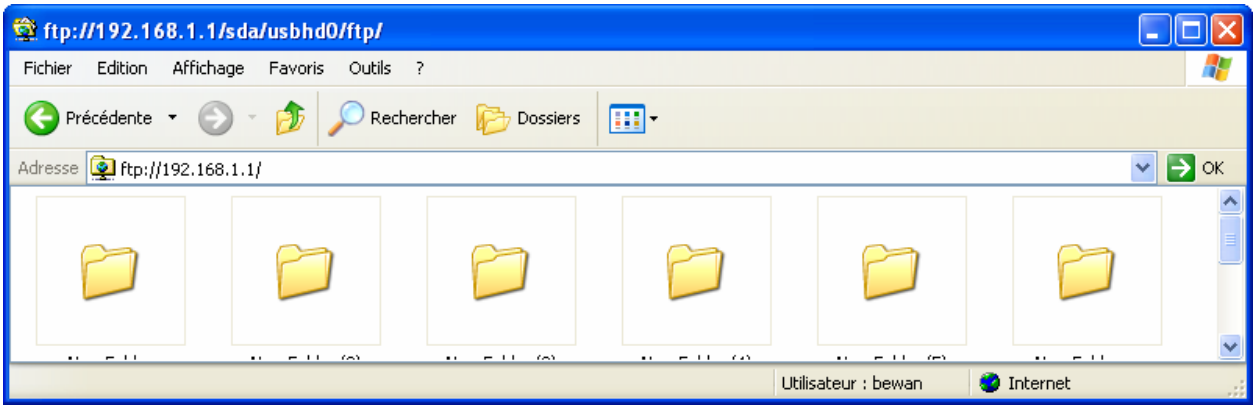
Ouvrez n'importe quel dossier de Windows XP (**Poste de travail**, par exemple) et saisissez l'adresse IP FTP dans le champ **Adresse**.



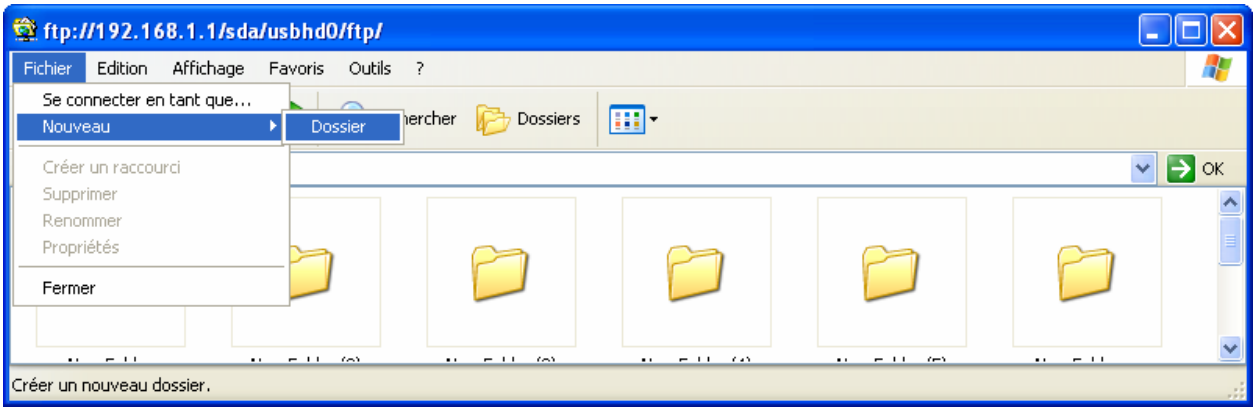
Lorsque vous appuyez sur **Entrée**, l'écran de connexion apparaît et vous invite à entrer le Nom d'utilisateur et le Mot de passe. Saisissez ces informations et cliquez sur **Ouvrir une session**. Si vous cochez l'option **Enregistrer le mot de passe**, vous n'aurez pas à entrer ce dernier lors de votre prochaine connexion.

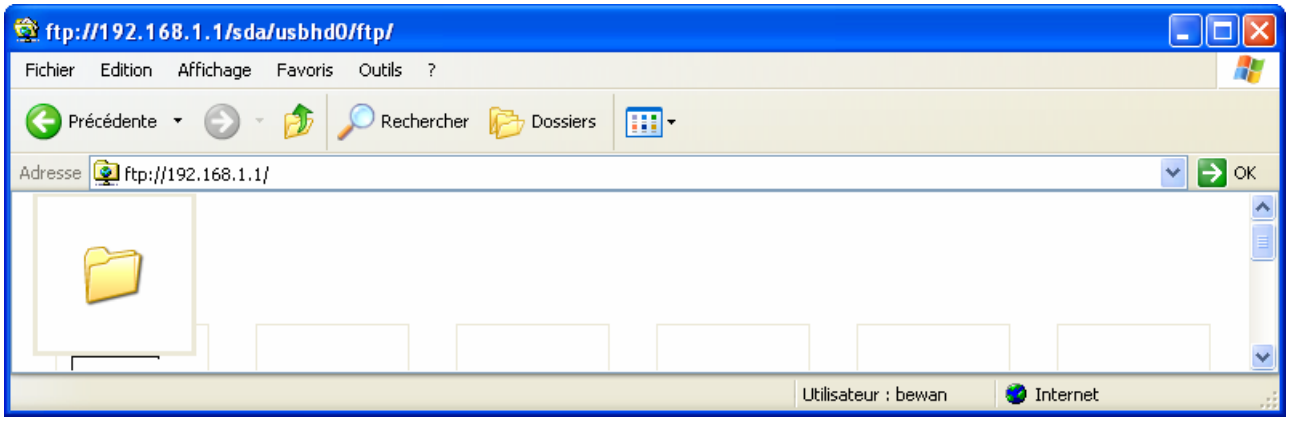

Ouvrir une session en tant que
Le serveur n'autorise pas les connexions anonymes, ou l'adresse de messagerie n'a pas été acceptée.
Serveur FTP : 192.168.1.1
Nom d'utilisateur : bewan
Mot de passe : •••••
Une fois que vous êtes connecté, vous pouvez ajouter ce serveur FTP à votre liste des Favoris et y revenir facilement.
FTP ne crypte pas ou ne code pas les mots de passe ou les données avant de les envoyer au serveur. Pour protéger la sécurité de vos mots de passe et des vos données, utilisez les dossiers Web (WebDAV) à la place.
En savoir plus sur l'utilisation des dossiers Web.
Ouvrir une session anonyme
Enregistrer le mot de passe
Ouvrir une session
Annuler

Connectez-vous au serveur FTP.



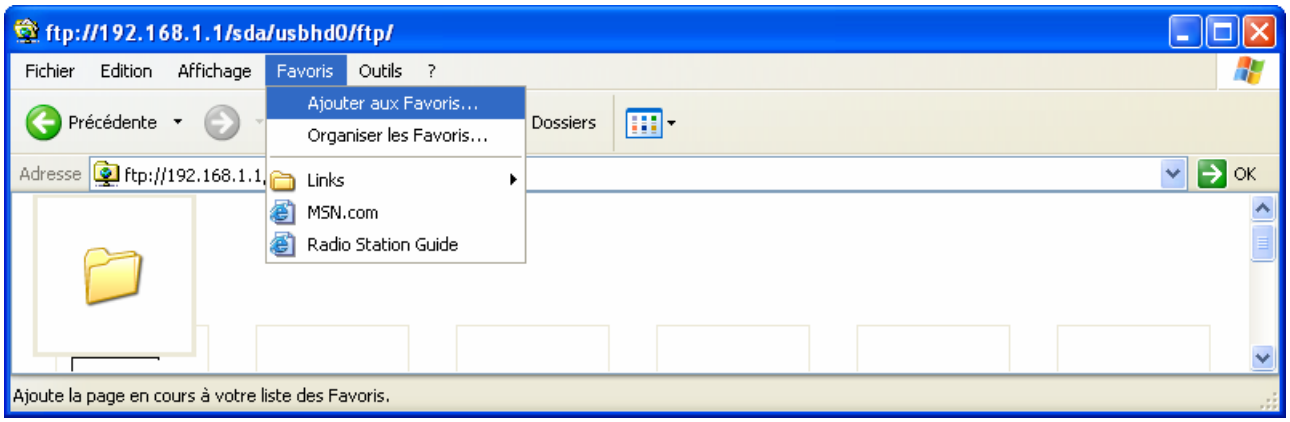
Créez maintenant le répertoire racine pour le compte FTP que nous allons créer par la suite. Sélectionnez **Nouveau** > **Dossier** dans le menu **Fichier**. Nommez le nouveau dossier.



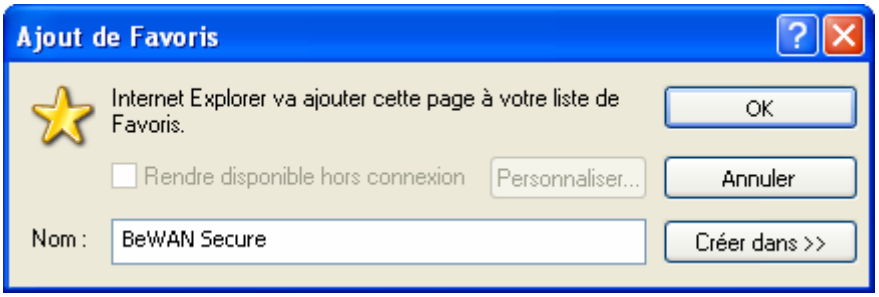


CREATION D'UN « VOISINAGE RESEAU » AVEC LE SERVEUR FTP

Si vous utilisez Windows 98, vous pouvez utiliser le voisinage réseau pour vous connecter au serveur FTP. Connectez-vous à la page Web du serveur FTP et sélectionnez **Ajouter aux favoris…** dans le menu **Favoris**.

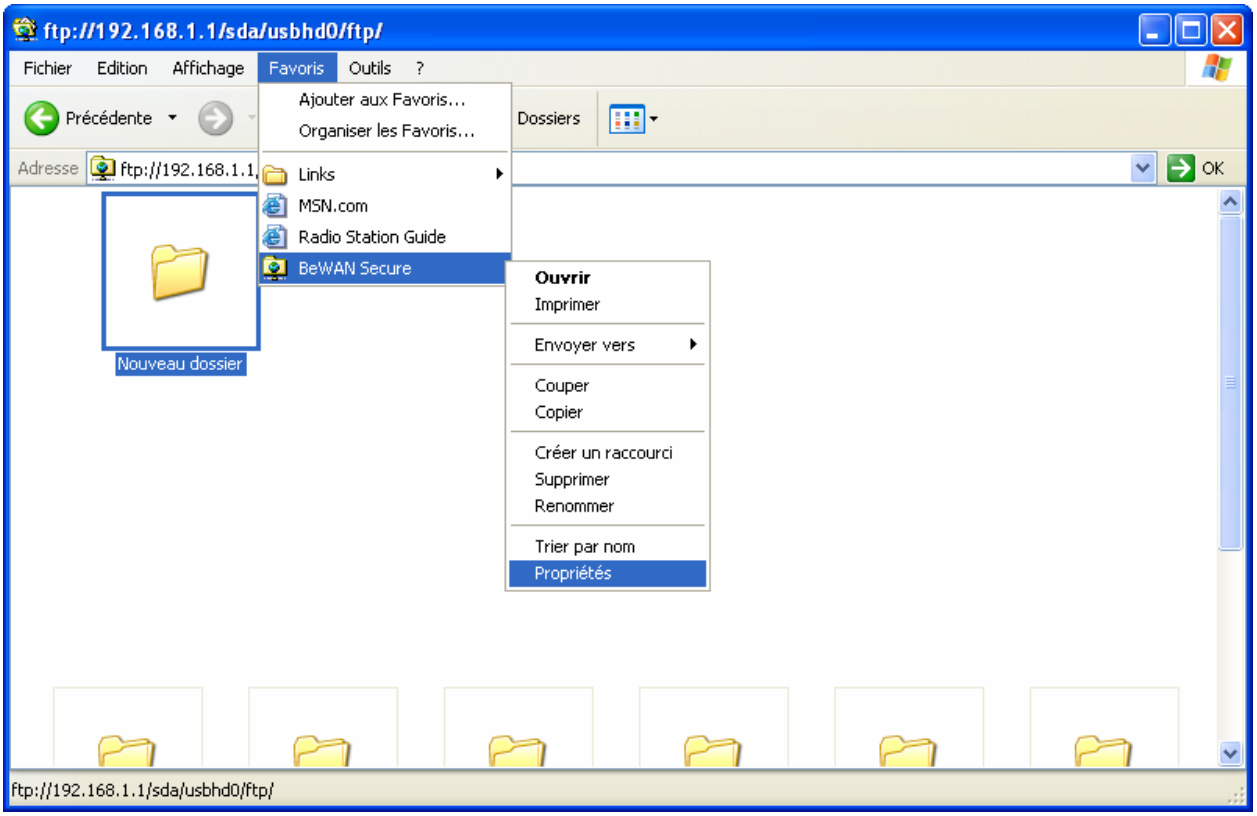


Modifiez le nom si nécessaire, puis cliquez sur **OK**.

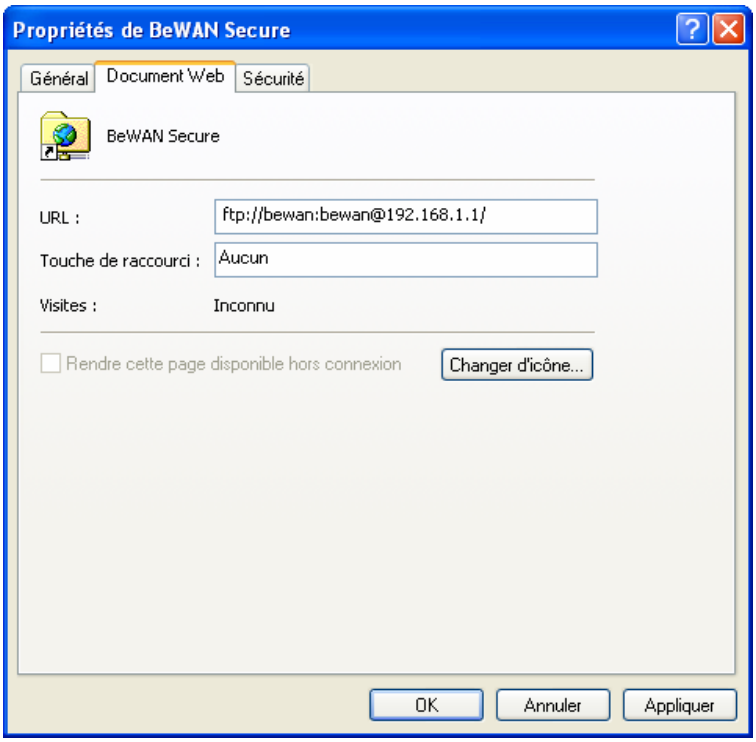


Sélectionnez ensuite **Organiser les favoris…** dans le menu **Favoris**.

Recherchez le nom du serveur FTP que vous venez d'ajouter aux **Favoris** et cliquez une fois dessus. Cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel.



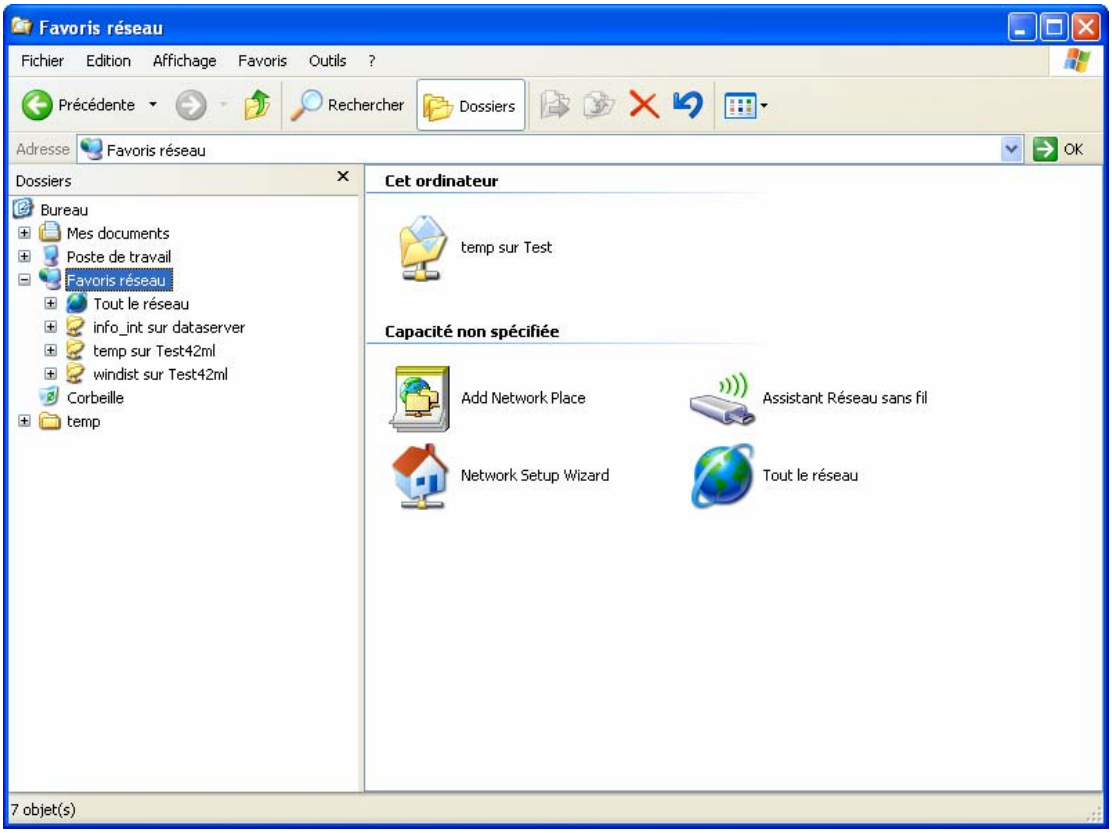
Cliquez sur **Propriétés**. La fenêtre ci-dessous s'ouvre.



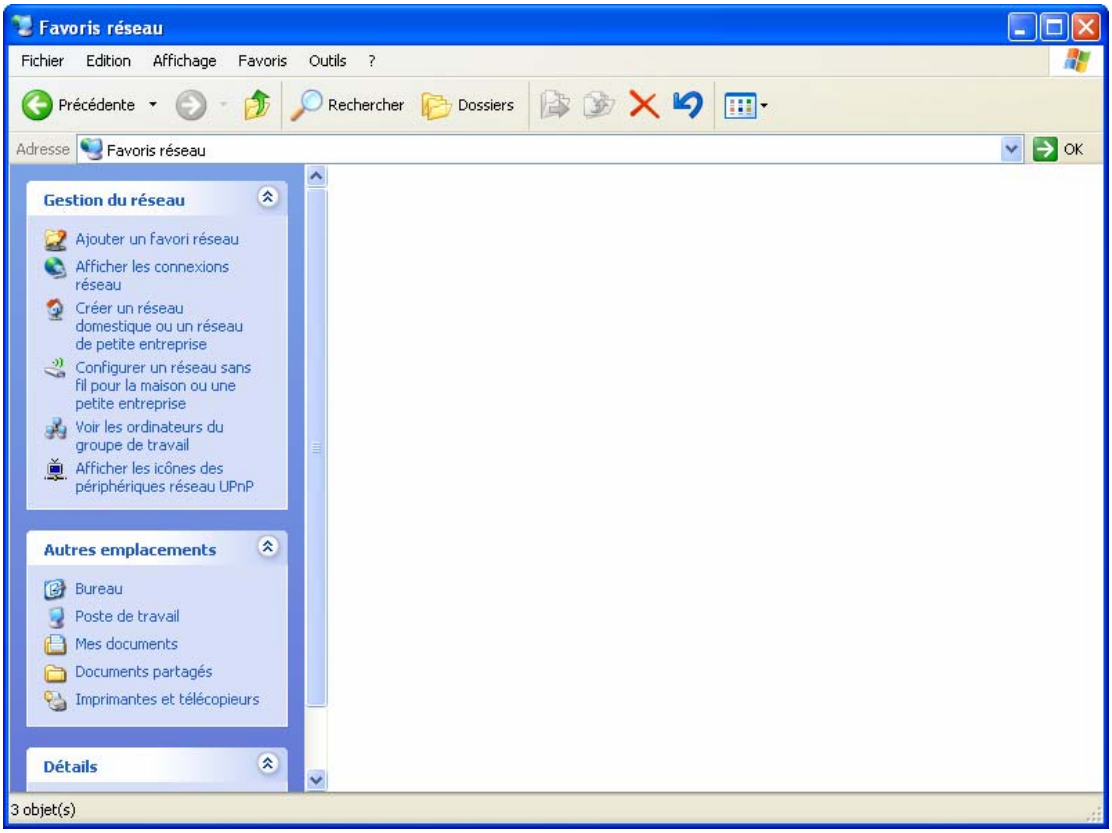
Cliquez sur **OK** pour terminer la configuration. Le dossier FTP apparaît désormais dans le voisinage réseau de l'Explorateur.

CREATION D'UN « VOISINAGE RESEAU » AVEC LE SERVEUR FTP (WIN 2000/XP)

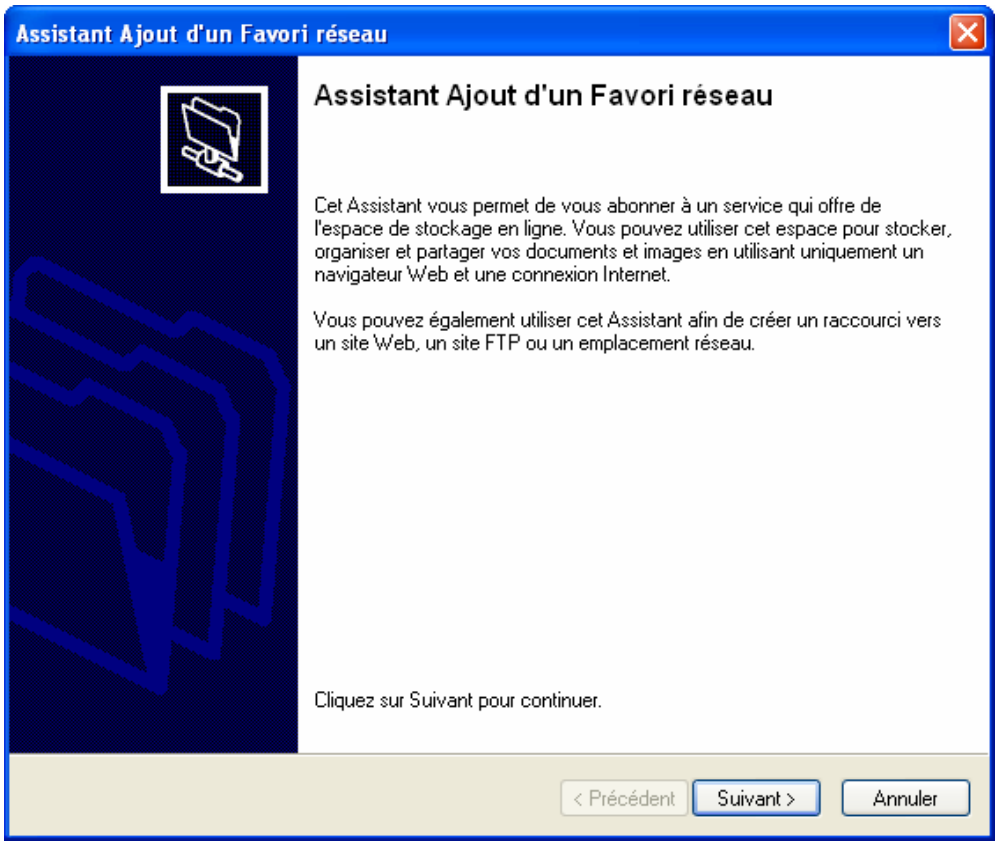
Ouvrez l'**Explorateur Windows** et cliquez sur **Voisinage réseau** ou **Favoris réseau**.



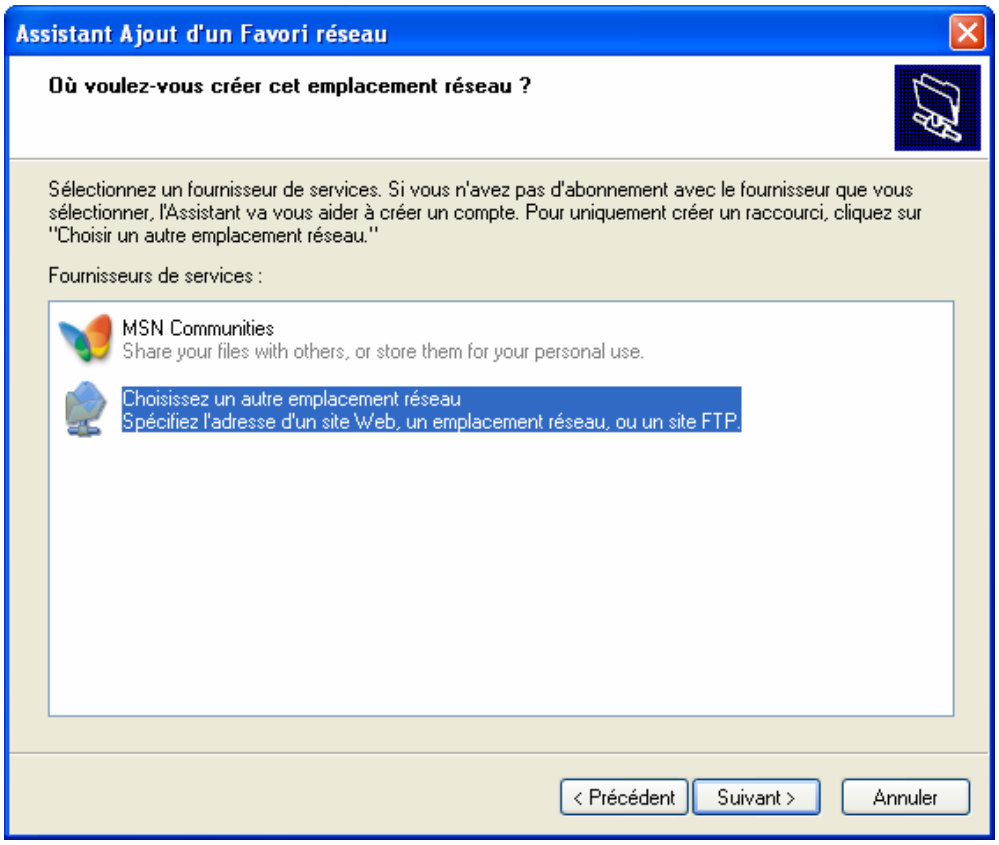
Vous trouverez dans cette fenêtre l'utilitaire appelé **Ajouter un favori réseau**.



Lorsque vous cliquez sur **Ajouter un favori réseau**, la page de bienvenue de l'assistant de configuration s'ouvre. Cliquez sur **Suivant** pour commencer la configuration.

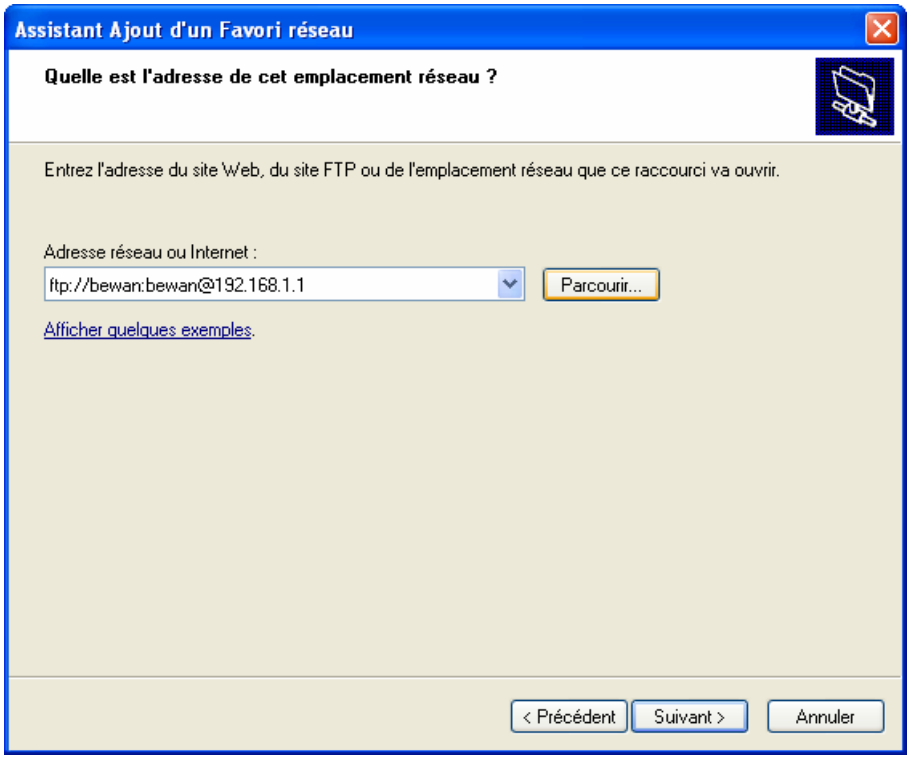

Assistant Ajout d'un Favori réseau
Assistant Ajout d'un Favori réseau
Cet Assistant vous permet de vous abonner à un service qui offre de l'espace de stockage en ligne. Vous pouvez utiliser cet espace pour stocker, organiser et partager vos documents et images en utilisant uniquement un navigateur Web et une connexion Internet.
Vous pouvez également utiliser cet Assistant afin de créer un raccourci vers un site Web, un site FTP ou un emplacement réseau.
Cliquez sur Suivant pour continuer.
< Précédent
Suivant >
Annuler

Cliquez à nouveau sur **Suivant** pour poursuivre la création du favori réseau à partir de cet emplacement FTP.

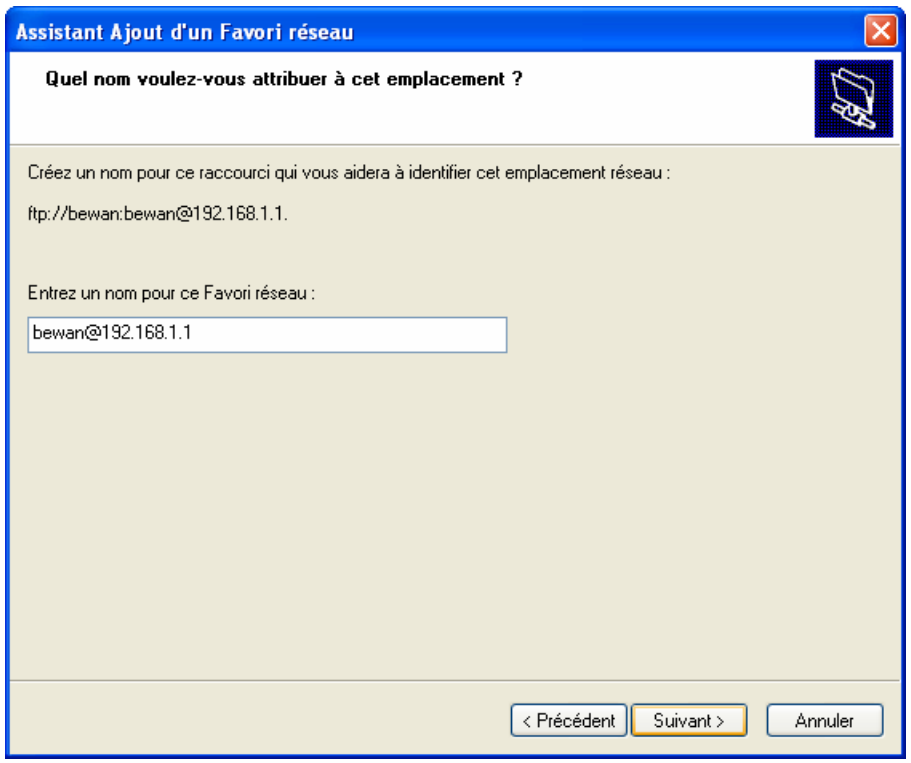

Assistant Ajout d'un Favori réseau
Où voulez-vous créer cet emplacement réseau ?
Sélectionnez un fournisseur de services. Si vous n'avez pas d'abonnement avec le fournisseur que vous sélectionner, l'Assistant va vous aider à créer un compte. Pour uniquement créer un raccourci, cliquez sur "Choisir un autre emplacement réseau."
Fournisseurs de services :
MSN Communities
Share your files with others, or store them for your personal use.
Choisissez un autre emplacement réseau
Spécifiez l'adresse d'un site Web, un emplacement réseau, ou un site FTP.
< Précédent
Suivant >
Annuler

Saisissez l'adresse FTP de l'emplacement pour lequel vous créez le favori réseau.

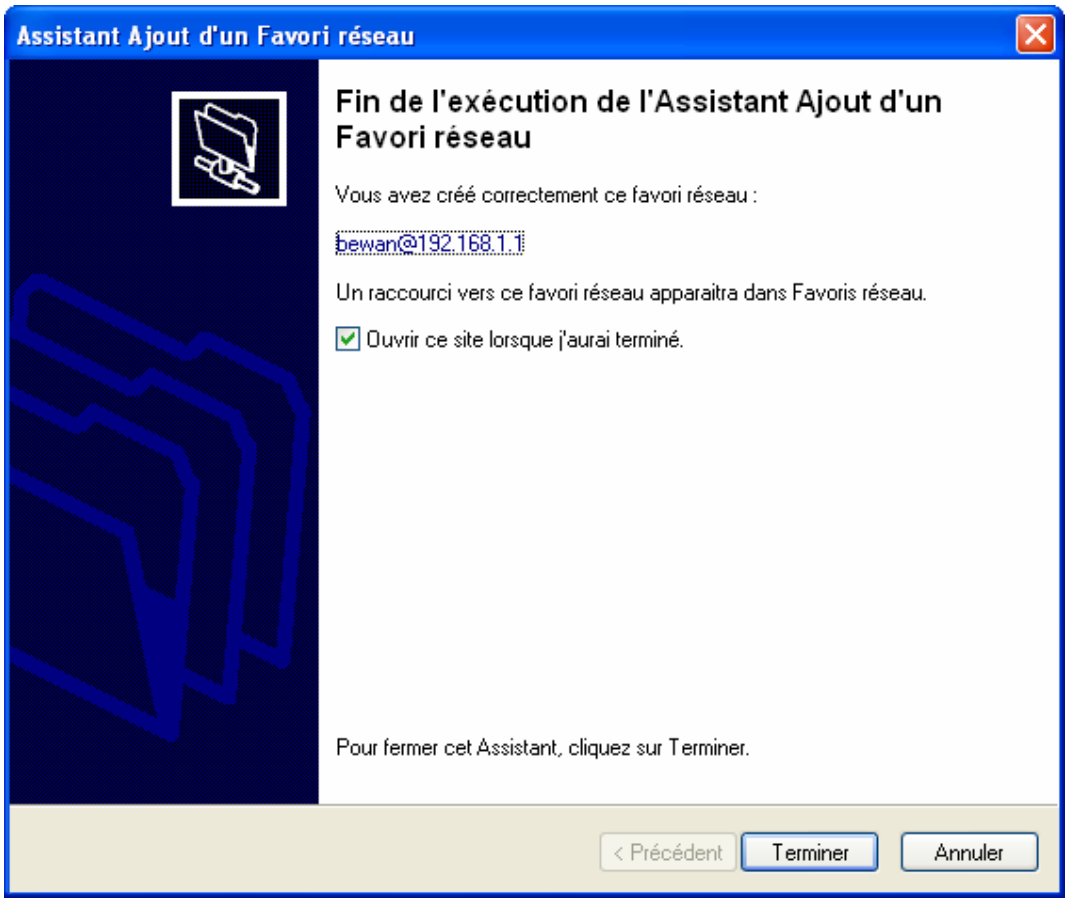
Astuce : pour éviter d'avoir à saisir le mot de passe à chaque accès au serveur FTP depuis les « Favoris réseau », il est recommandé d'ajouter le mot de passe dans l'adresse IP FTP pour que les autres utilisateurs n'aient pas à le saisir de nouveau lorsqu'ils accèdent au serveur depuis votre réseau local. L'adresse FTP devrait être de la forme : ftp://Nom-du-compte:Mot-de-passe@Adresse IP WAN.


Assistant Ajout d'un Favori réseau
Quelle est l'adresse de cet emplacement réseau ?
Entrez l'adresse du site Web, du site FTP ou de l'emplacement réseau que ce raccourci va ouvrir.
Adresse réseau ou Internet :
ftp://bewan:bewan@192.168.1.1
Parcourir...
Afficher quelques exemples.
< Précédent
Suivant >
Annuler

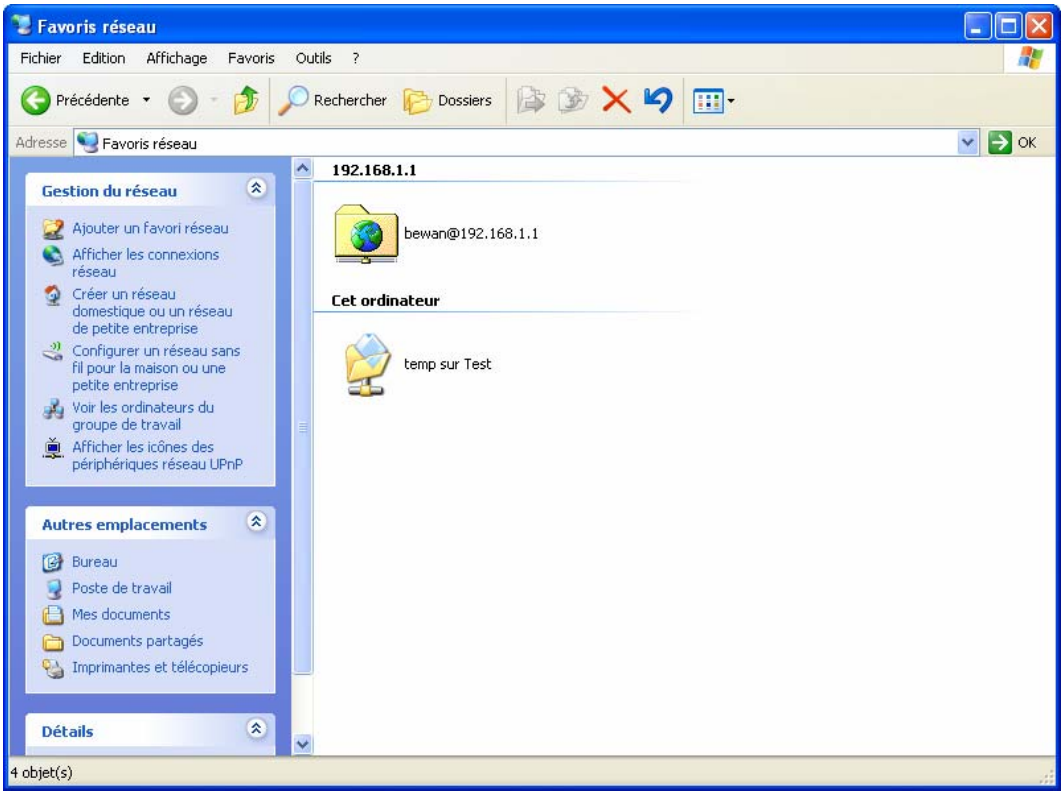
Sur cette page, vous devez saisir le nom du serveur FTP tel qu'il apparaîtra dans les **Favoris réseau**. Cliquez sur **Suivant** pour continuer.


Assistant Ajout d'un Favori réseau
Quel nom voulez-vous attribuer à cet emplacement ?
Créez un nom pour ce raccourci qui vous aidera à identifier cet emplacement réseau :
ftp://bewan:bewan@192.168.1.1.
Entrez un nom pour ce Favori réseau :
bewan@192.168.1.1
< Précédent
Suivant >
Annuler

La configuration est maintenant terminée. Cliquez sur **Terminer** pour quitter l'assistant de configuration.

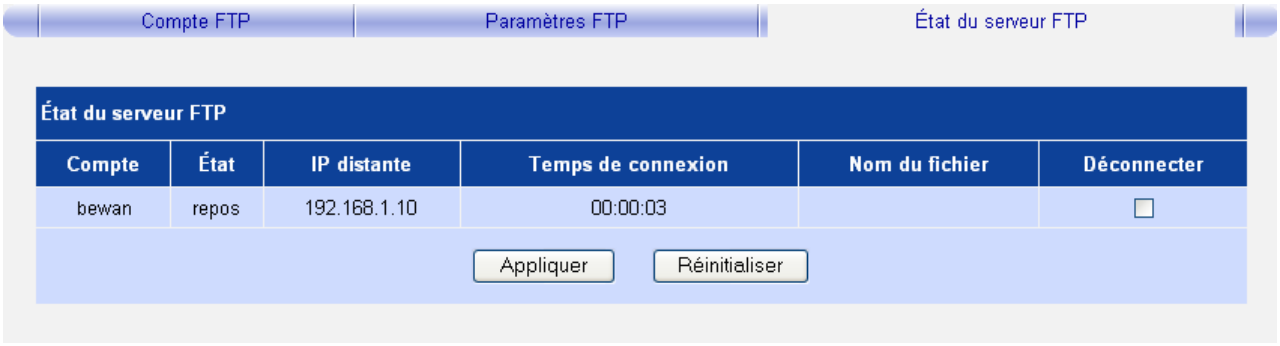

Assistant Ajout d'un Favori réseau
Fin de l'exécution de l'Assistant Ajout d'un Favori réseau
Vous avez créé correctement ce favori réseau :
bewan@192.168.1.1
Un raccourci vers ce favori réseau apparaitra dans Favoris réseau.
Ouvrir ce site lorsque j'aurai terminé.
Pour fermer cet Assistant, cliquez sur Terminer.
< Précédent
Terminer
Annuler

Retournez maintenant dans l'**Explorateur Windows** et ouvrez les Favoris réseau. Le dossier du serveur FTP devrait s'y trouver.



État du serveur FTP

Cliquez sur **Serveur FTP** dans le menu principal, puis sur **État du serveur FTP**. Vous pouvez vérifier ici l'état des connexions au serveur FTP.



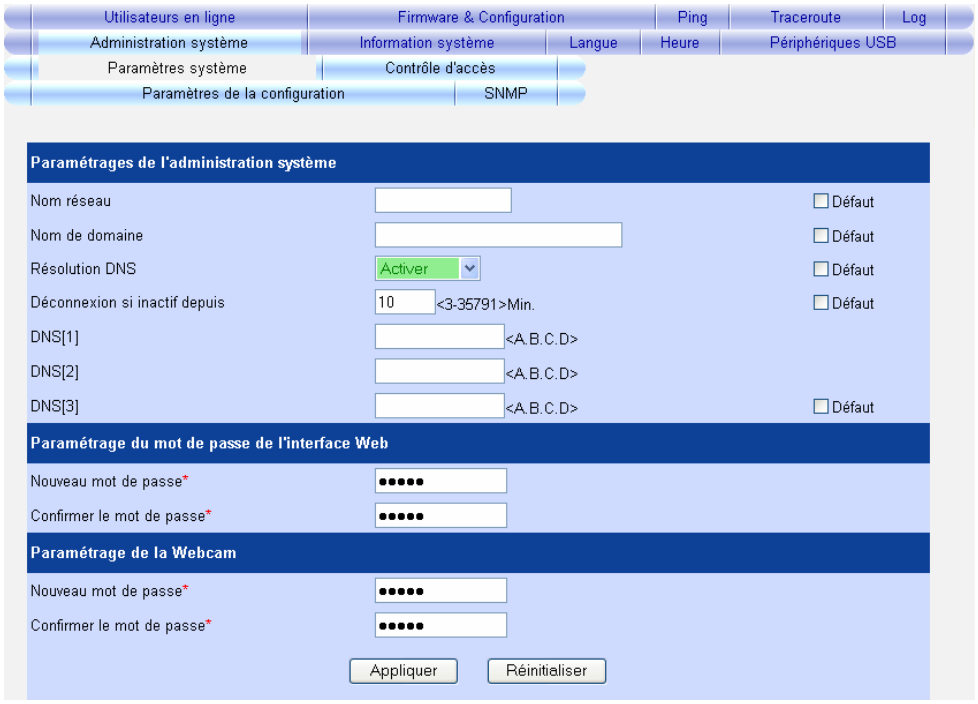
Pour déconnecter un utilisateur, cochez la case **Déconnecter** correspondante et cliquez sur le bouton **Appliquer**. Cliquez sur **Réinitialiser** pour annuler la sélection.

Maintenance

Les options de configuration et les outils relatifs au fonctionnement du système en lui-même se trouvent dans Maintenance.

Administration système

Les options de configuration de cette section se rapportent toutes au fonctionnement et à la gestion de base du système.



Nom réseau

Le nom du système dans le réseau. Si, par exemple, le nom complet du réseau est utilisateur.home.net, le nom du réseau est utilisateur.

Nom de domaine

Le nom du domaine où se situe le système. Si, par exemple, le nom complet du réseau est utilisateur.home.net, le nom de domaine est home.net.

Résolution DNS

Sélectionnez **Activer** ou **Désactiver**.

Déconnexion si inactif depuis

Si vous n'effectuez aucune opération de gestion dans cet intervalle de temps, le système vous déconnecte automatiquement.

DNS[1]

Indiquez le nom de votre serveur de noms de domaine (DNS). Si votre type de connexion au réseau étendu peut lui-même obtenir l'adresse du serveur DNS, ou si vous êtes sûr de ne pas vouloir utiliser de serveur DNS, vous pouvez laisser ce champ vide.

DNS[2]

Voir ci-dessus.

DNS[3]

Voir ci-dessus.

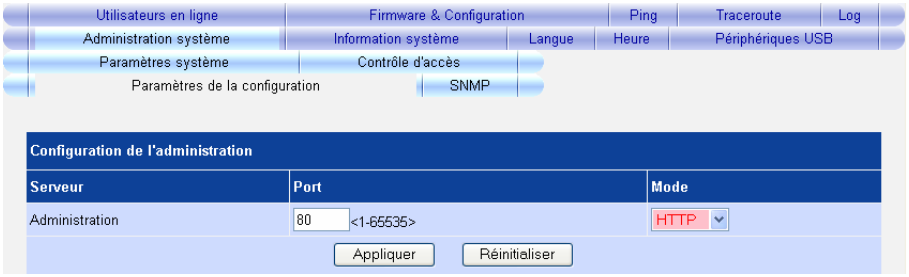
Paramétrage du mot de passe

Définissez le mot de passe de l'interface d'administration Web.

Cliquez sur **Appliquer** pour que les paramètres du système soient pris en compte. Cliquez sur **Réinitialiser** pour annuler les modifications.

PARAMETRES DE LA CONFIGURATION

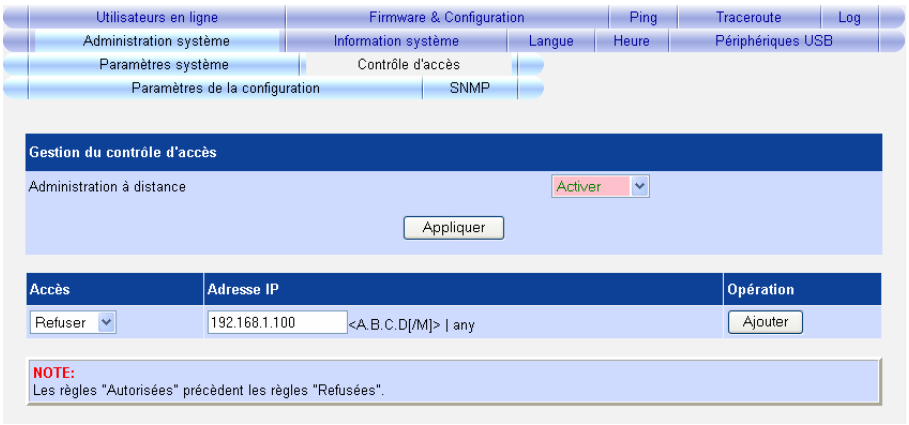
Cliquez sur **Maintenance** dans le menu principal de gauche, puis sur **Administration Système** > **Paramètres de la configuration** pour spécifier le serveur Web et le numéro de port utilisé par l'interface d'administration Web, ainsi que le protocole utilisé : HTTP (non crypté) ou HTTPS (crypté).



Cliquez sur **Appliquer** pour que les modifications soient prises en compte. Cliquez sur **Réinitialiser** pour annuler les modifications.

CONTROLE D'ACCES

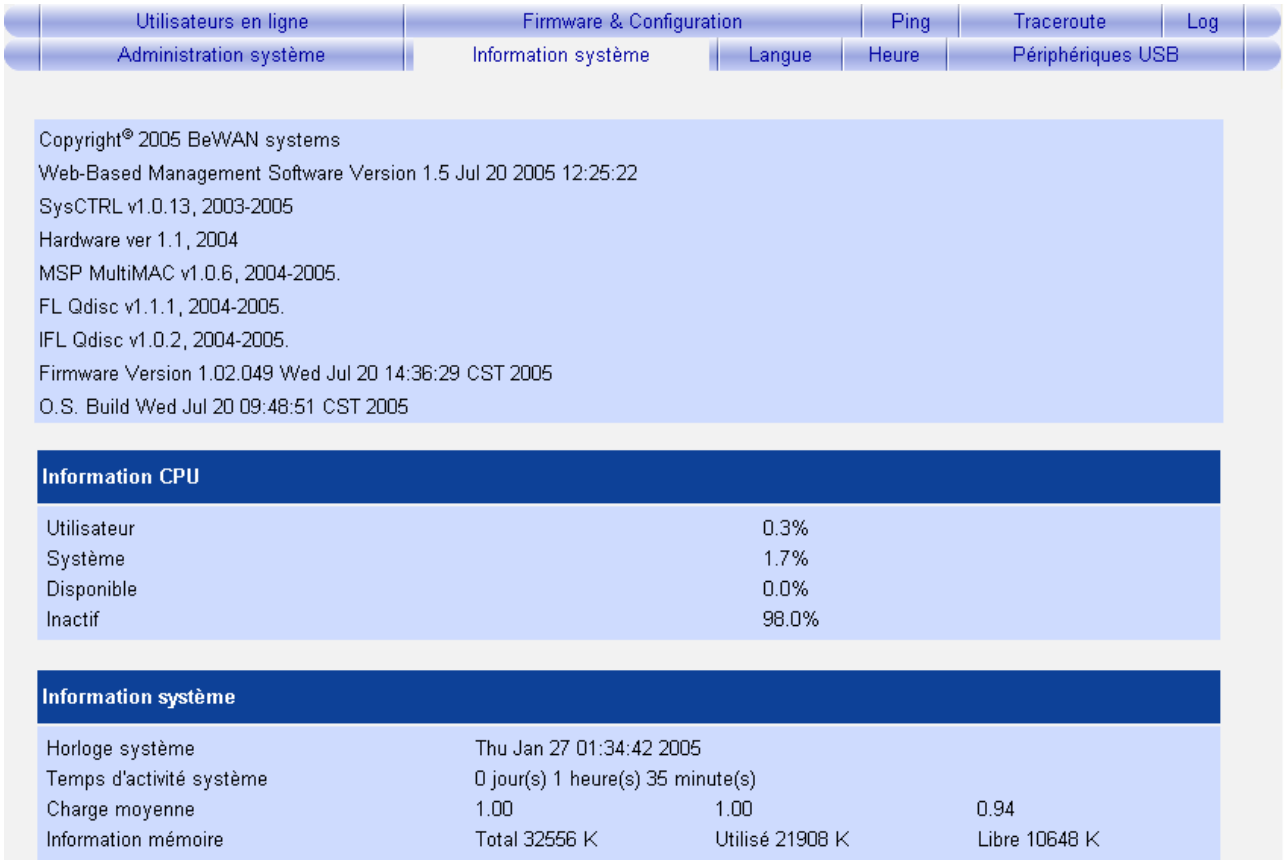
Cliquez sur **Maintenance** dans le menu principal de gauche, puis sur **Administration système** > **Contrôle d'accès** pour autoriser ou refuser la connexion à l'hôte ou au sous-réseau. .any. représente tous les périphériques.



Cliquez sur **Appliquer** pour activer la fonction Administration à distance. Cliquez sur **Ajouter** pour ajouter une règle de contrôle d'accès.

Information système

Cette page fournit la version du firmware ainsi que des informations concernant le processeur (CPU) et le système d'exploitation. Voir ci-dessous.

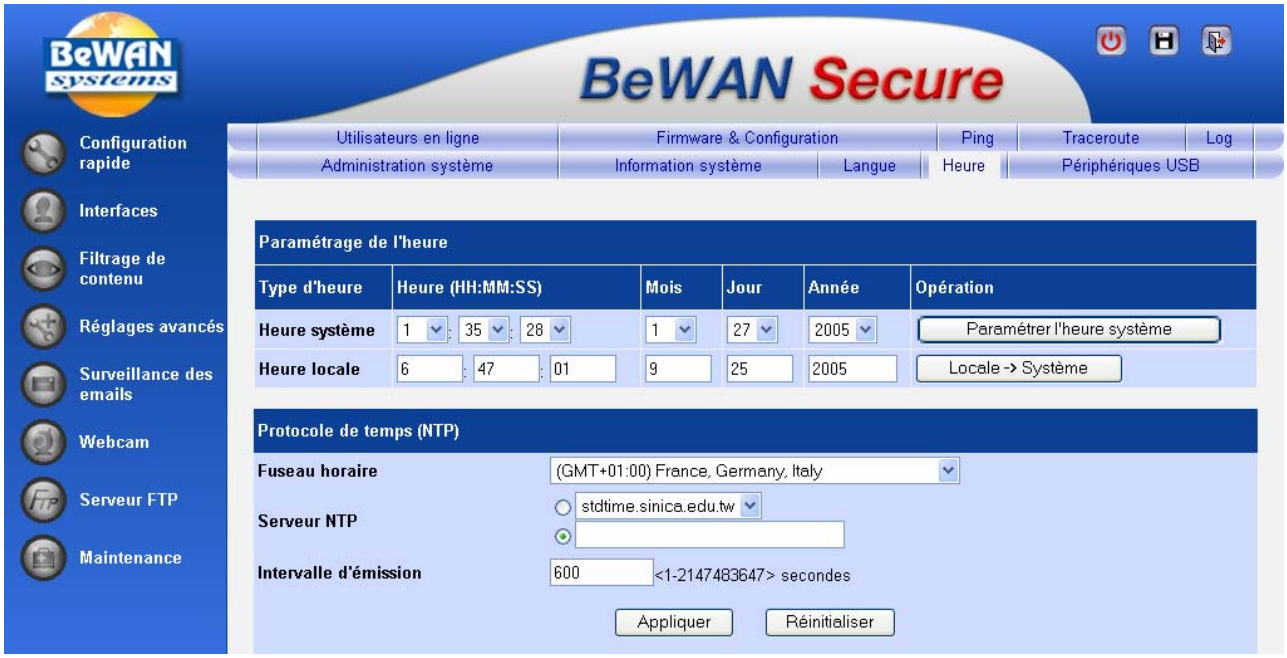


Langue

Le système prend en charge une interface en anglais et en français, avec possibilité de basculement à tout moment. Sélectionnez la langue et cliquez sur **Appliquer**. Le système bascule immédiatement vers la langue sélectionnée.

Heure

Utilisez cette page pour définir le fuseau horaire, l'heure système, le serveur NTP, etc.



Heure système

Définissez manuellement l'heure du système.

Heure locale

Appliquez l'heure locale à l'heure système. L'heure locale est l'heure de l'ordinateur que vous utilisez.

Fuseau horaire

Le fuseau horaire dans lequel vous vous trouvez.

Serveur NTP

Spécifiez un serveur NTP. Vous pouvez le sélectionner dans la liste par défaut ou entrer directement son adresse IP ou son nom. Si vous ne souhaitez pas configurer de serveur NTP, sélectionnez la zone de saisie manuelle et laissez-la vide.

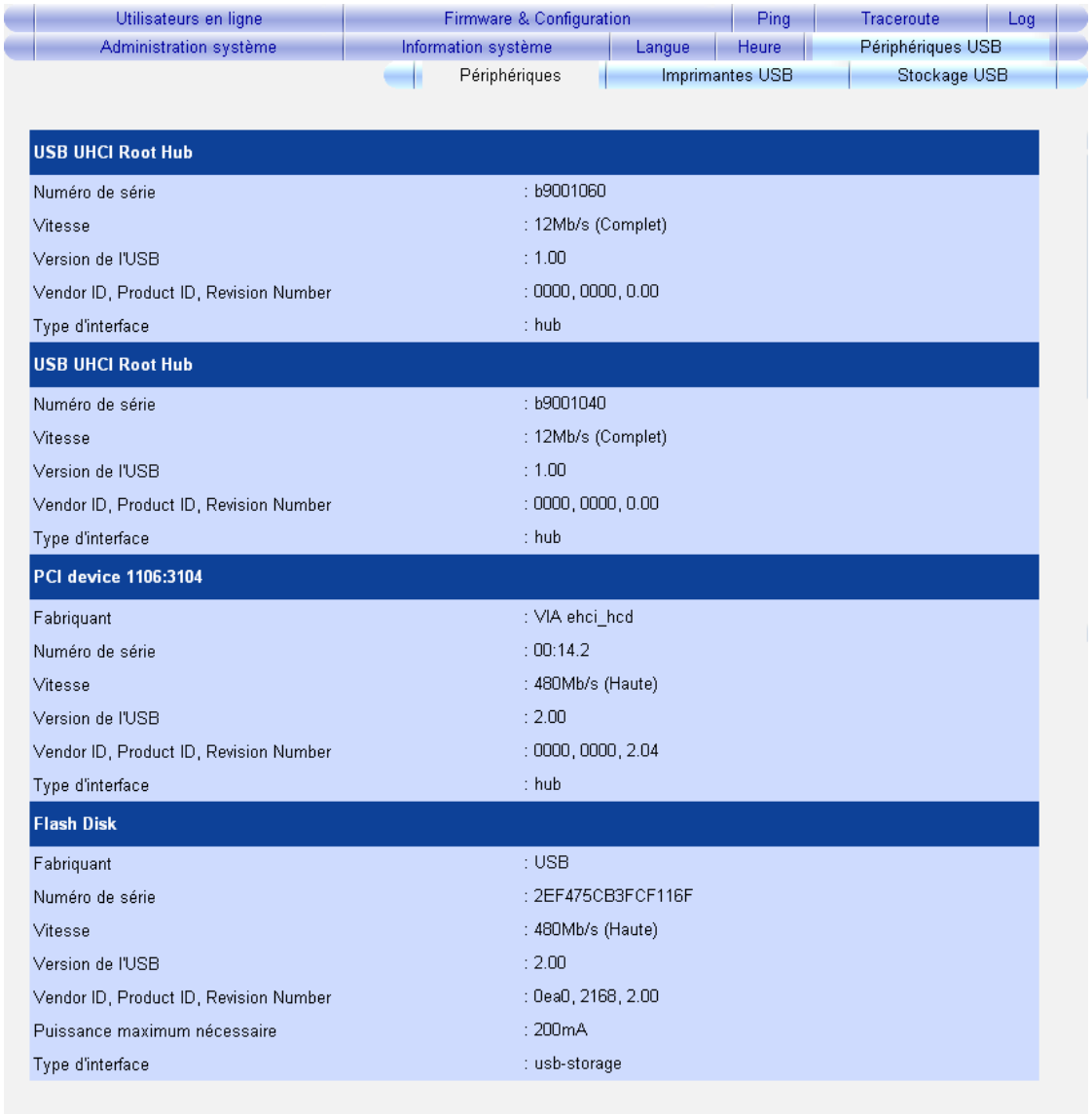
Intervalle d'émission

La fréquence à laquelle le système interroge le serveur NTP.

Les trois derniers paramètres doivent être activés en cliquant sur le bouton **Appliquer**. Vous pouvez cliquer sur le bouton **Réinitialiser** pour annuler les modifications.

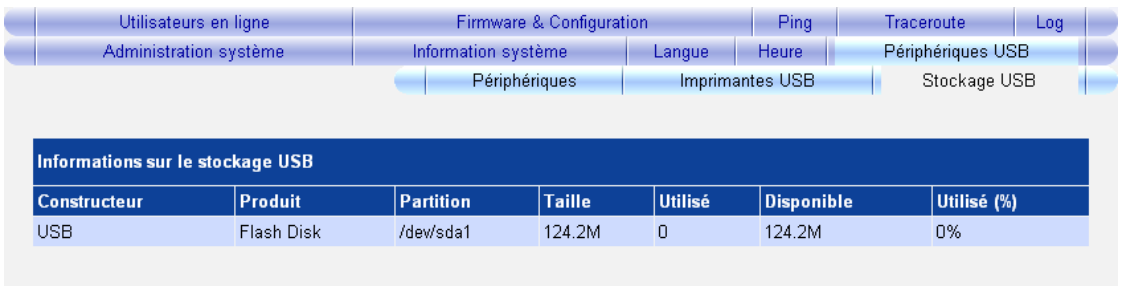
Périphériques USB

Cliquez sur **Périphériques USB** pour afficher les périphériques USB actuellement connectés au système. Cette section contient également les informations détaillées relatives aux imprimantes USB et aux périphériques de stockage USB.

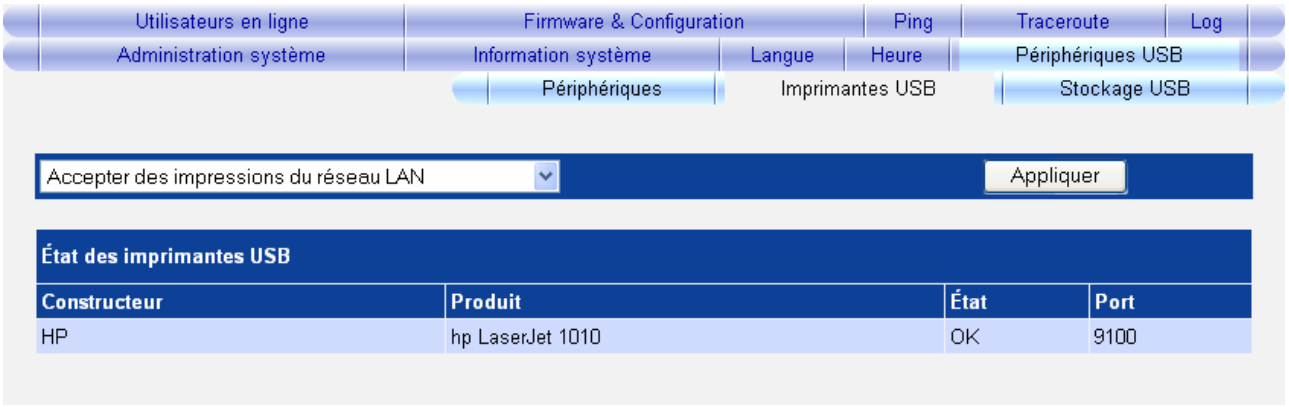

Utilisateurs en ligne
Firmware & Configuration
Ping
Traceroute
Log
Administration système
Information système
Langue
Heure
Périphériques USB
Périphériques
Imprimantes USB
Stockage USB
USB UHCI Root Hub
Numéro de série : b9001060
Vitesse : 12Mb/s (Complet)
Version de l'USB : 1.00
Vendor ID, Product ID, Revision Number : 0000, 0000, 0.00
Type d'interface : hub
USB UHCI Root Hub
Numéro de série : b9001040
Vitesse : 12Mb/s (Complet)
Version de l'USB : 1.00
Vendor ID, Product ID, Revision Number : 0000, 0000, 0.00
Type d'interface : hub
PCI device 1106:3104
Fabriquant : VIA ehci_hcd
Numéro de série : 00:14.2
Vitesse : 480Mb/s (Haute)
Version de l'USB : 2.00
Vendor ID, Product ID, Revision Number : 0000, 0000, 2.04
Type d'interface : hub
Flash Disk
Fabriquant : USB
Numéro de série : 2EF475CB3FCF116F
Vitesse : 480Mb/s (Haute)
Version de l'USB : 2.00
Vendor ID, Product ID, Revision Number : 0ea0, 2168, 2.00
Puissance maximum nécessaire : 200mA
Type d'interface : usb-storage

Comme l'indique la capture d'écran ci-dessus, un périphérique de stockage USB est connecté au système. Ces informations peuvent également être consultées dans la section Stockage USB.

Cliquez sur **Imprimantes USB** pour afficher les informations relatives aux imprimantes USB. Veuillez également sélectionner ici le réseau sur lequel les imprimantes sont partagées.



Cliquez sur **Stockage USB** pour afficher les informations relatives aux périphériques de stockage USB. Les détails de ces derniers figurent sur cette page. Vous pouvez voir les partitions, la taille, la quantité d'espace utilisé, etc.



Utilisateurs en ligne

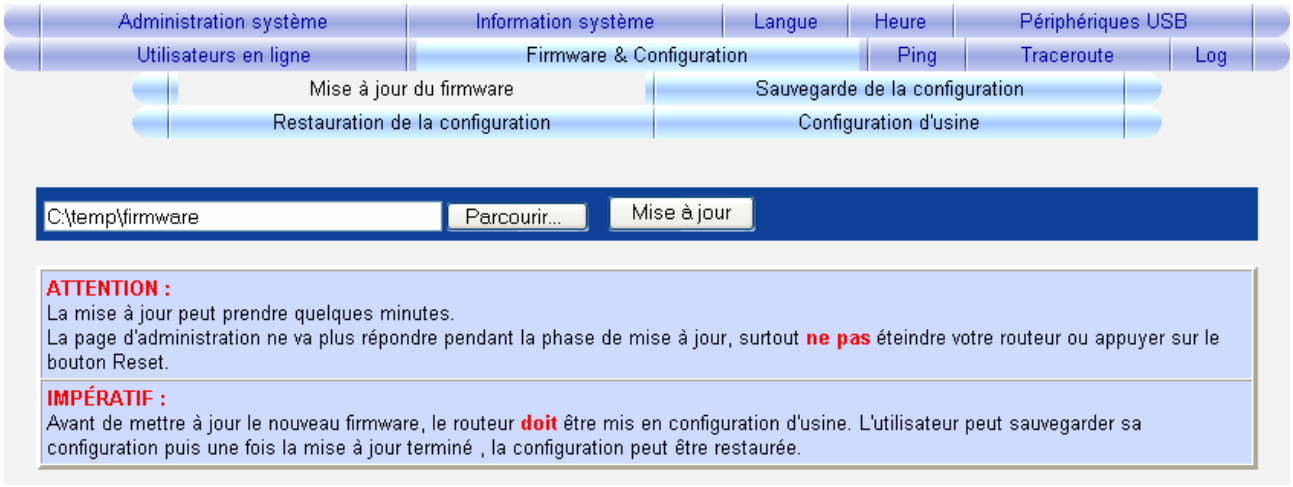
Cette page affiche les utilisateurs connectés à l'interface d'administration Web. Le système n'autorise que trois utilisateurs à se connecter simultanément à cette interface. Cochez la case **Déconnecter** et cliquez sur le bouton **Appliquer** pour déconnecter un utilisateur.

Firmware & Configuration

La page **Firmware & Configuration** comporte quatre sections : Mise à jour du firmware, Restauration de la configuration, Sauvegarde de la configuration et Configuration d'usine.

MISE A JOUR DU FIRMWARE

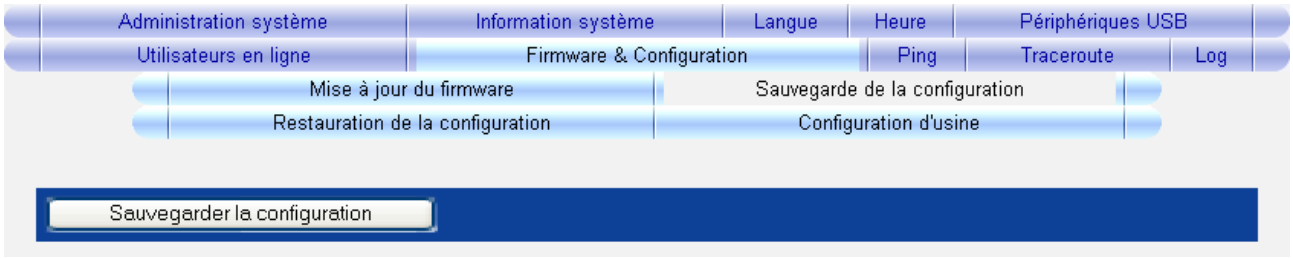
Utilisez cette page pour mettre à jour le firmware. Veuillez vous reporter à l'illustration ci-dessous pour effectuer la mise à jour.


Administration système
Information système
Langue
Heure
Périphériques USB
Utilisateurs en ligne
Firmware & Configuration
Ping
Traceroute
Log
Mise à jour du firmware
Sauvegarde de la configuration
Restauration de la configuration
Configuration d'usine
C:\temp\firmware
Parcourir...
Mise à jour
ATTENTION :
La mise à jour peut prendre quelques minutes.
La page d'administration ne va plus répondre pendant la phase de mise à jour, surtout ne pas éteindre votre routeur ou appuyer sur le bouton Reset.
IMPÉRATIF :
Avant de mettre à jour le nouveau firmware, le routeur doit être mis en configuration d'usine. L'utilisateur peut sauvegarder sa configuration puis une fois la mise à jour terminé , la configuration peut être restaurée.

Cliquez sur le bouton **Parcourir…** de la section **Mise à jour du firmware**. L'explorateur affiche la liste des fichiers. Sélectionnez d'abord le firmware stocké sur l'hôte d'administration. Cliquez ensuite sur le bouton **Mise à jour** pour mettre à jour le firmware du système. Le système commence par vérifier l'intégrité du fichier du firmware. Il ne commence la mise à jour qu'après avoir effectué cette vérification. Pendant la mise à jour, le voyant **Status** clignote. L'opération dure environ 5 minutes. Après la mise à jour, le système redémarre automatiquement. Veillez à débrancher et à rebrancher l'appareil à ce moment-là.

SAUVEGARDE DE LA CONFIGURATION

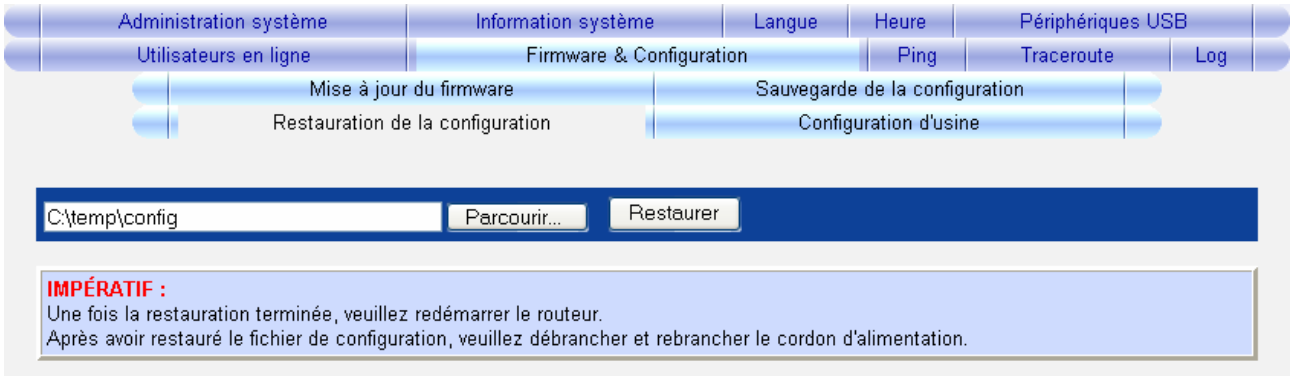
Utilisez cette page pour sauvegarder le fichier de configuration du système. Veuillez vous reporter à l'illustration ci-dessous pour effectuer la sauvegarde.



Le système vous permet de sauvegarder et de restaurer le fichier de configuration. Cliquez sur le bouton **Sauvegarder la configuration**. L'explorateur vous invite à indiquer l'emplacement où vous souhaitez stocker le fichier. Sélectionnez ou saisissez le nom du nouveau fichier. Le fichier de configuration est enregistré sur l'hôte d'administration sous le nom indiqué.

RESTAURATION DE LA CONFIGURATION

Utilisez cette page pour restaurer le fichier de configuration du système. Veuillez vous reporter à l'illustration ci-dessous pour effectuer la restauration.

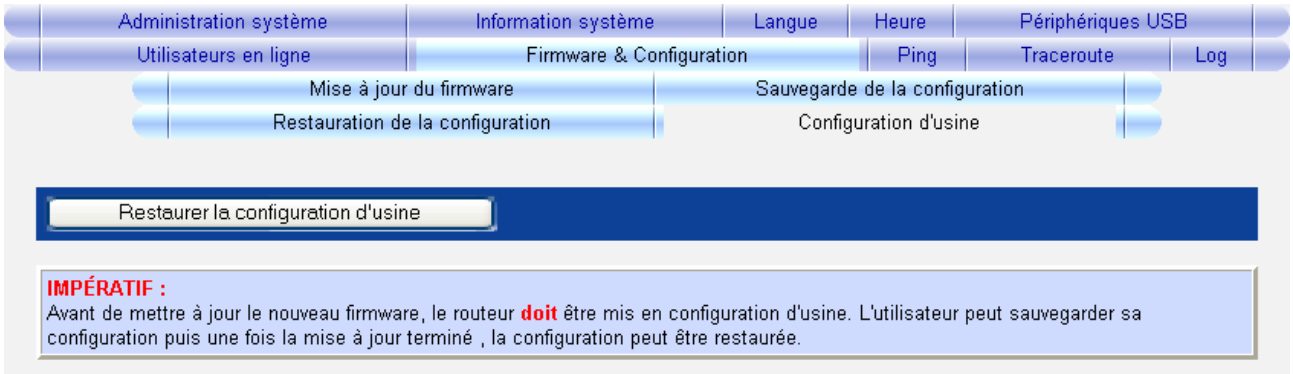


Pour restaurer la configuration, cliquez sur le bouton **Parcourir…** de la section **Restauration de la configuration**, sélectionnez le fichier, puis cliquez sur le bouton **Restaurer**. Une fois la restauration terminée, redémarrez le système.

Remarque : après avoir restauré le fichier de configuration du système, débranchez et rebranchez l'appareil.

CONFIGURATION D'USINE

Utilisez cette page pour restaurer la configuration définie en usine. Veuillez vous reporter à l'illustration ci-dessous pour effectuer la réinitialisation.


Administration système
Information système
Langue
Heure
Périphériques USB
Utilisateurs en ligne
Firmware & Configuration
Ping
Traceroute
Log
Mise à jour du firmware
Sauvegarde de la configuration
Restauration de la configuration
Configuration d'usine
Restaurer la configuration d'usine
IMPÉRATIF :
Avant de mettre à jour le nouveau firmware, le routeur doit être mis en configuration d'usine. L'utilisateur peut sauvegarder sa configuration puis une fois la mise à jour terminé , la configuration peut être restaurée.

Cliquez sur le bouton **Restaurer la configuration d'usine**. Le système vous invite à confirmer l'opération.

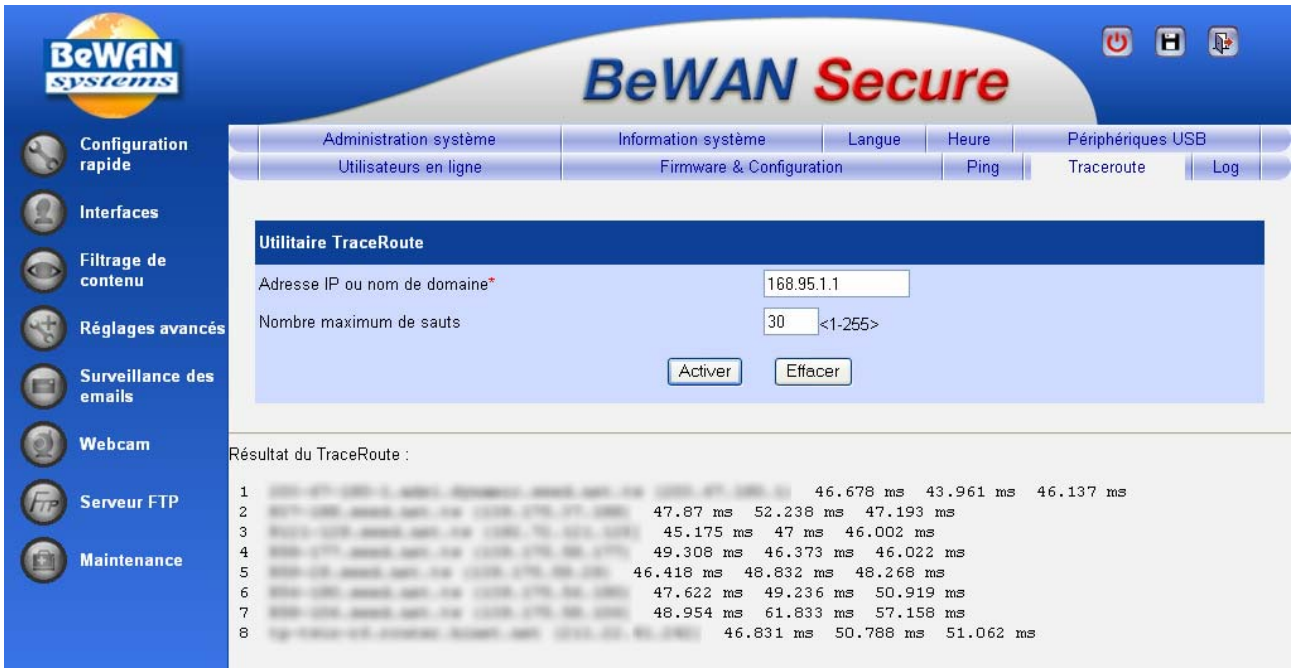
Ping

L'outil Ping permet de tester l'état de la connexion du routeur et de l'hôte affecté. Renseignez le champ **Adresse IP ou nom de domaine** ; si vous le souhaitez, vous pouvez également définir l'adresse source et le nombre de tentatives. Cliquez sur le bouton **Activer** pour commencer le test.

Une fois le test terminé, le système affiche les résultats de ce dernier.

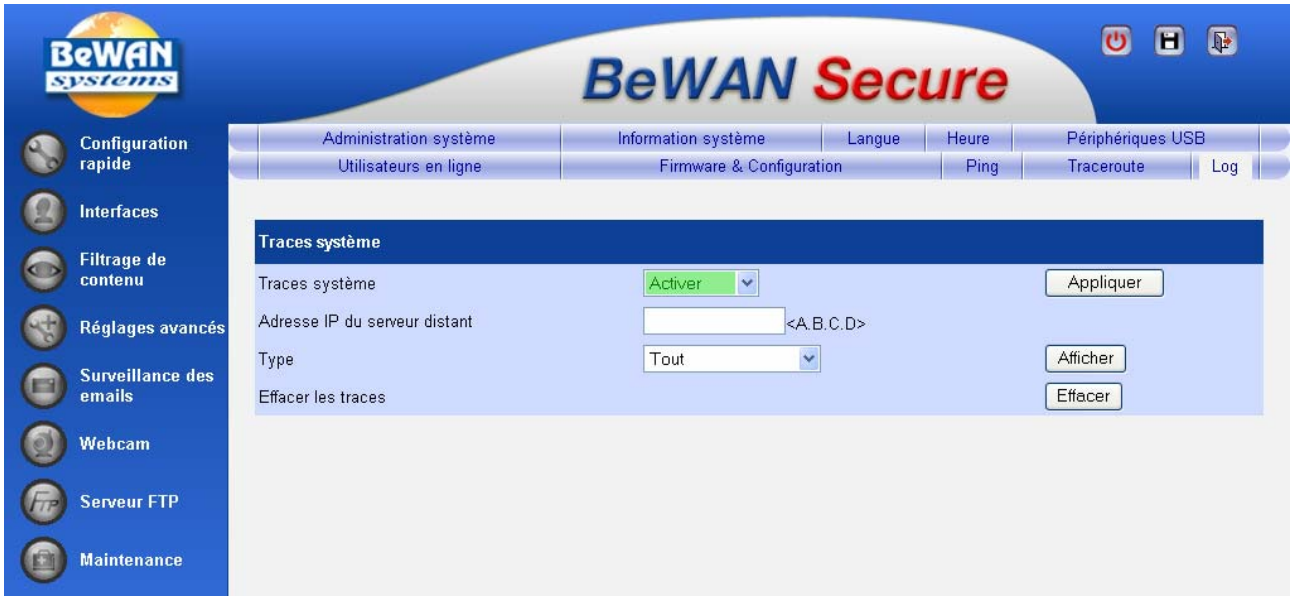
Traceroute

L'outil Ping ne fournit que l'état de la connexion avec l'hôte cible. Si vous ne parvenez pas à vous connecter à cet hôte, vous pouvez utiliser l'outil TraceRoute pour connaître l'état de l'envoi et le chemin emprunté.

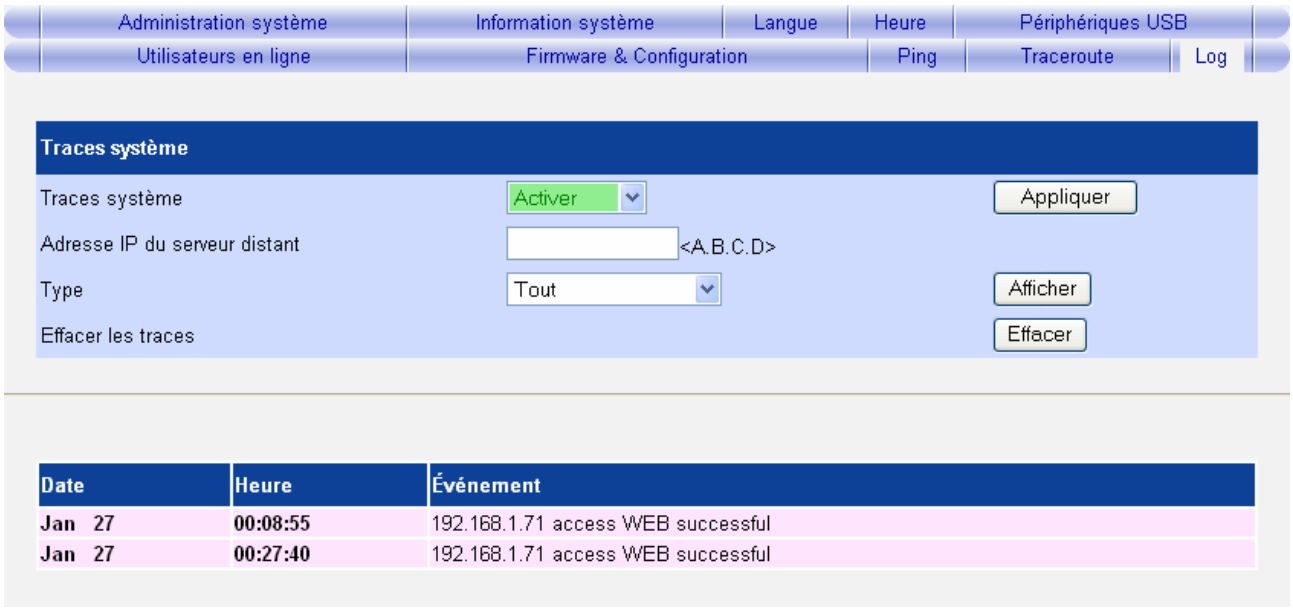


Log

La fonction **Log** enregistre en détail les événements système. Vous pouvez l'activer ou la désactiver, effacer les traces ou filtrer par type les événements à afficher.



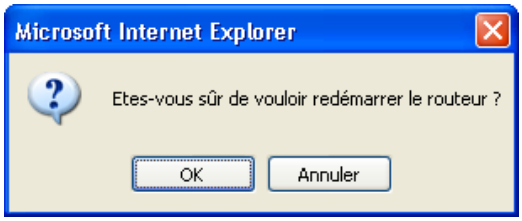
Les types d'événements pouvant être affichés sont les suivants : Tout, Pare-feu, Système, Entrant, Sortant, Filtre de contenu et IPSec.



Si la liste des résultats filtrés tient sur plusieurs pages, vous pouvez sélectionner le numéro de page dans la liste déroulante prévue à cet effet. Vous pouvez également cliquer sur le bouton **Suivant** pour afficher la page suivante.

Redémarrer

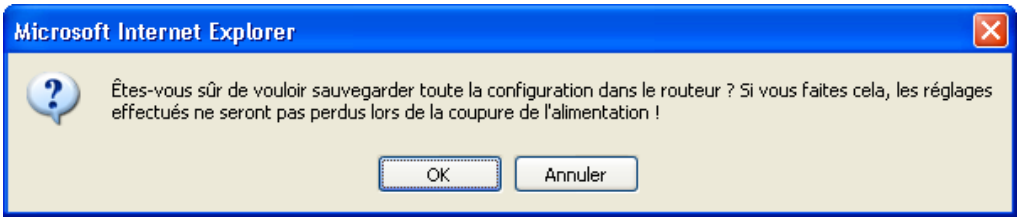
Si vous avez effectué des modifications mais que vous souhaitez restaurer les configurations précédemment sauvegardées, vous pouvez cliquer sur l'icône **Redémarrer**. Le système vous invite à confirmer le redémarrage du routeur.



Si vous cliquez sur **OK**, le système redémarre immédiatement. Toute configuration modifiée non sauvegardée sera perdue.

Sauvegarder

Si vous avez modifié la configuration du système et souhaitez conserver les paramètres après le redémarrage du système, cliquez sur l'icône **Sauvegarder** dans le coin supérieur droit de la fenêtre. Le système vous invite à confirmer la sauvegarde des paramètres.


Microsoft Internet Explorer
Êtes-vous sûr de vouloir sauvegarder toute la configuration dans le routeur ? Si vous faites cela, les réglages effectués ne seront pas perdus lors de la coupure de l'alimentation !
OK
Annuler

Si vous cliquez sur le bouton **OK**, le système sauvegarde la configuration et affiche le résultat de la sauvegarde après quelques secondes.

Déconnecter

Cliquez sur l'icône **Déconnecter** dans le coin supérieur droit de la fenêtre pour vous déconnecter de l'interface d'administration Web.

5. Serveur d'impression (sous Windows 2000 et XP)

Les modèles BeWAN Secure M50 et M50G sont dotés de 4 ports USB 2.0 intégrés pour faciliter la connexion et le partage avec une large gamme de périphériques USB. Ils permettent donc notamment de partager une ou plusieurs imprimantes (jusqu'à quatre imprimantes peuvent être partagées simultanément sur votre réseau) et font office de serveur d'impression. Il vous suffit de connecter votre imprimante.

Procédez comme indiqué ci-dessous pour configurer votre PC en vue d'une connexion à un serveur d'impression.

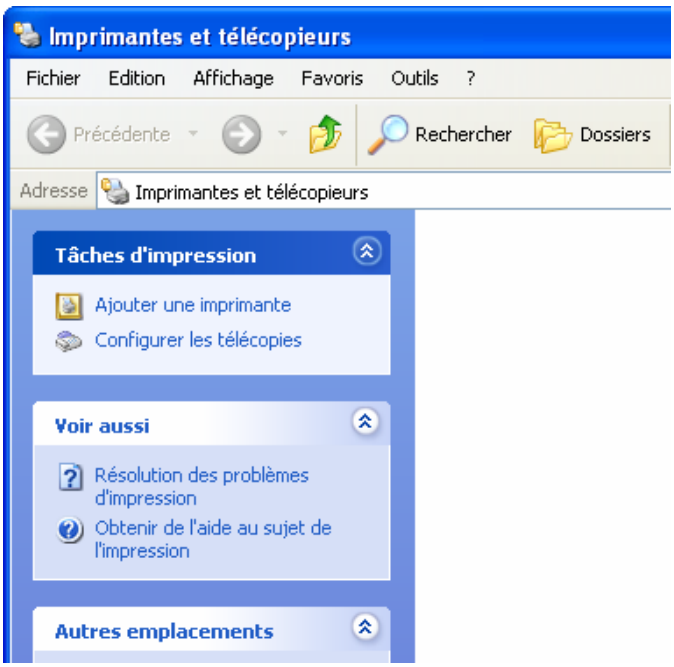
Pour installer un serveur d'impression, vous devez connaître son adresse IP et son numéro de port. L'adresse IP est l'adresse IP de l'interface LAN du routeur.

1. Connectez l'imprimante au système et sélectionnez **Maintenance** > **Périphériques USB** > **Imprimantes USB** pour connaître l'adresse IP. Supposons que le numéro de port soit 9100.
2. Une fois l'imprimante USB connectée reconnue par le système, cliquez sur **Sauvegarder** pour que ce dernier mémorise le numéro de port utilisé par cette imprimante.

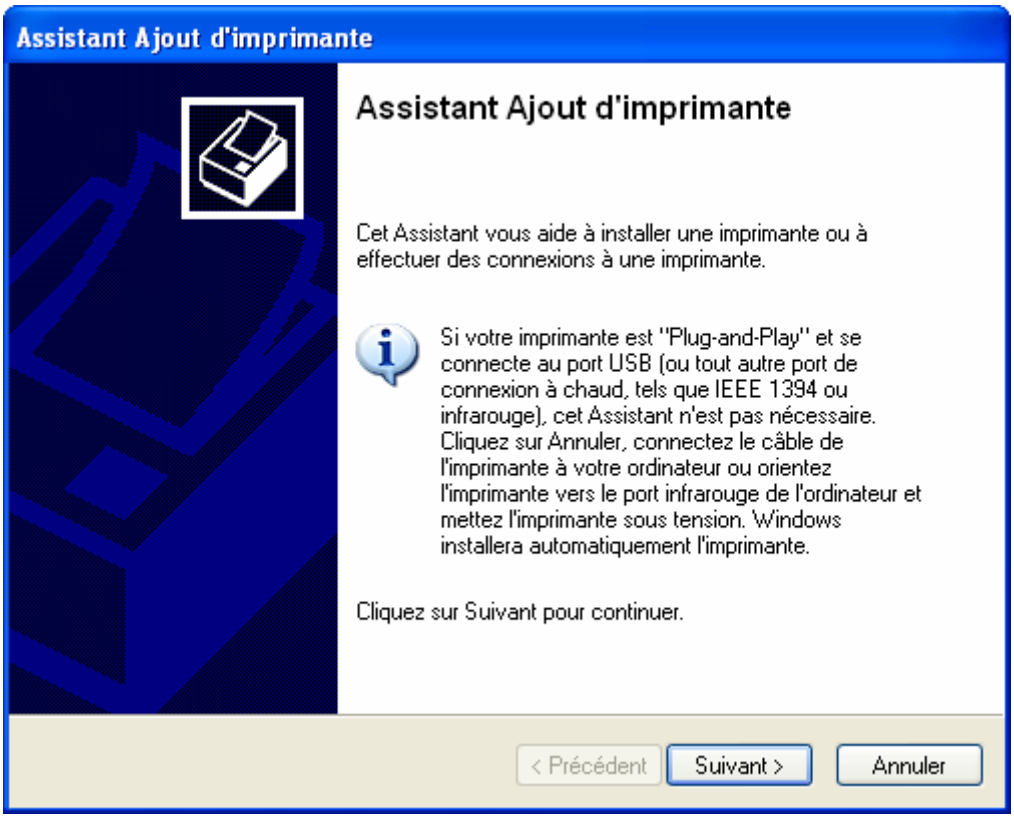
Remarque : à moins d'utiliser une imprimante différente de la même marque et avec un numéro de série identique, vous devez toujours déconnecter l'imprimante et la reconnecter au redémarrage du système pour qu'elle utilise le numéro de port précédemment mémorisé. Si vous déconnectez l'imprimante reconnue avant d'avoir enregistré les modifications et que vous la reconnectez par la suite, il se peut qu'elle utilise un autre numéro de port.

Après avoir raccordé votre imprimante au routeur, vous devez désormais configurer les ordinateurs de votre réseau local en installant sur chaque poste les pilotes de votre imprimante. Procédez comme suit :

1. Cliquez sur **démarrer > Panneau de configuration > Imprimantes et télécopieurs**.
2. Cliquez sur **Ajouter une imprimante**.

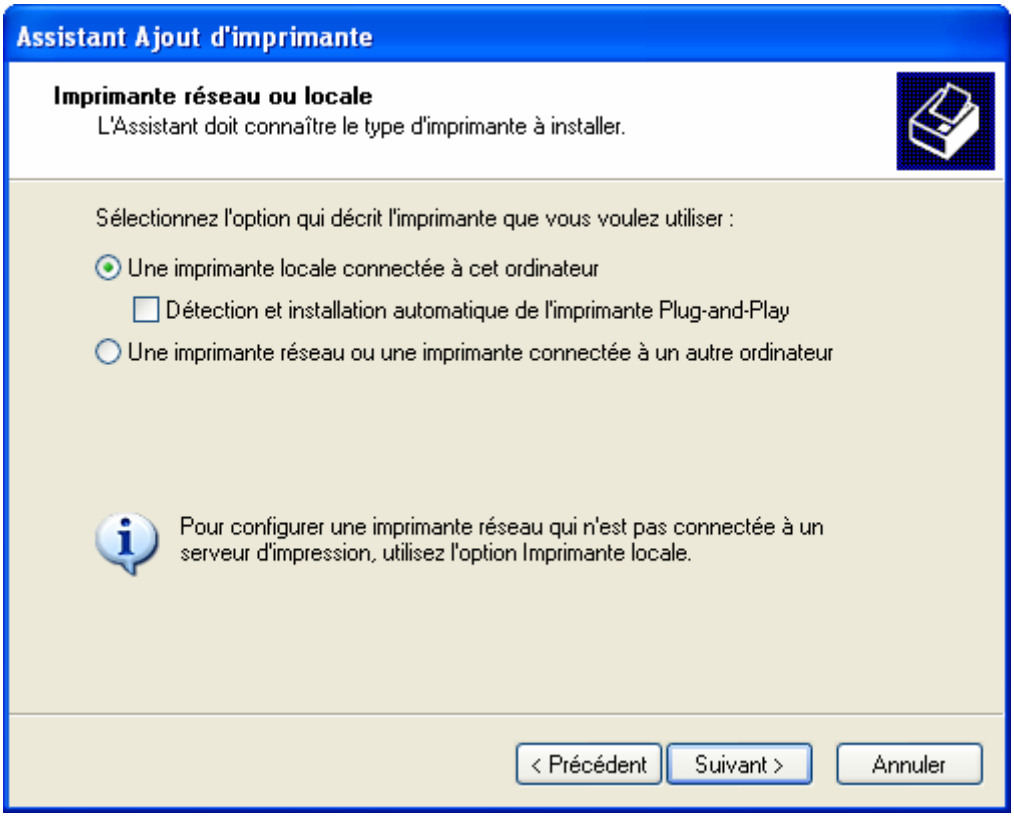


3. L'**Assistant Ajout d'imprimante** apparaît. Cliquez sur **Suivant**.

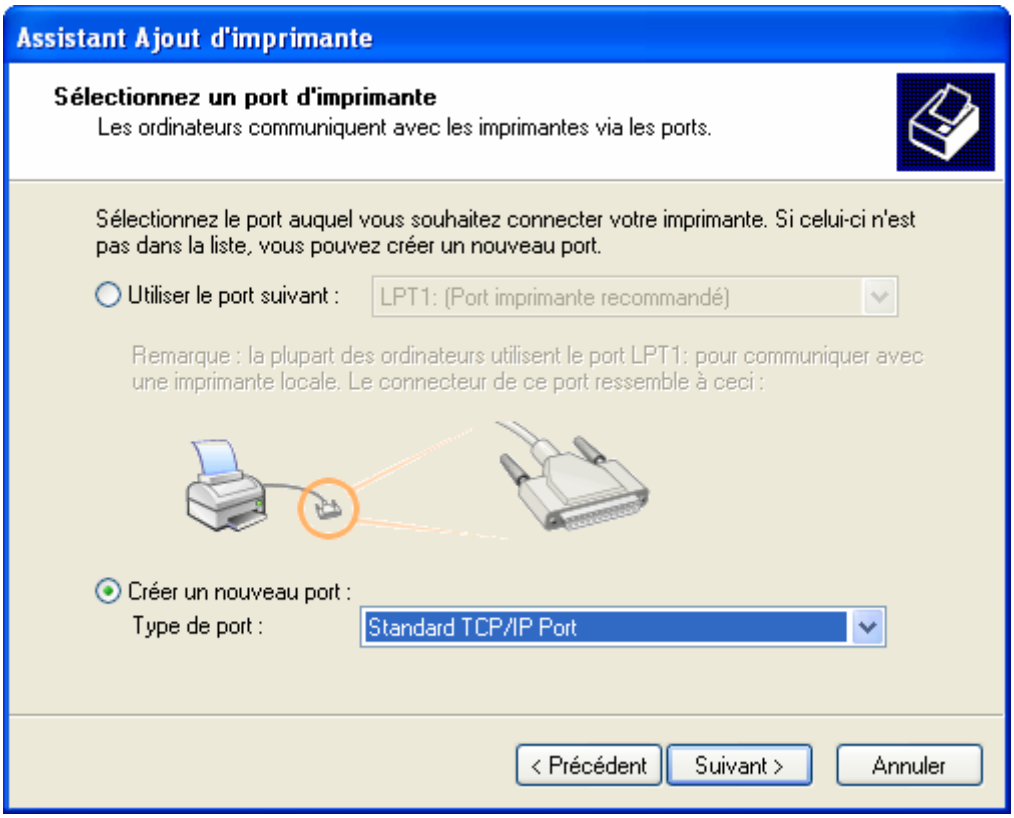

Assistant Ajout d'imprimante
Assistant Ajout d'imprimante
Cet Assistant vous aide à installer une imprimante ou à effectuer des connexions à une imprimante.
Si votre imprimante est "Plug-and-Play" et se connecte au port USB (ou tout autre port de connexion à chaud, tels que IEEE 1394 ou infrarouge), cet Assistant n'est pas nécessaire. Cliquez sur Annuler, connectez le câble de l'imprimante à votre ordinateur ou orientez l'imprimante vers le port infrarouge de l'ordinateur et mettez l'imprimante sous tension. Windows installera automatiquement l'imprimante.
Cliquez sur Suivant pour continuer.
< Précédent
Suivant >
Annuler

4. Sélectionnez **Une imprimante locale connectée à cet ordinateur**, puis cliquez sur **Suivant**.

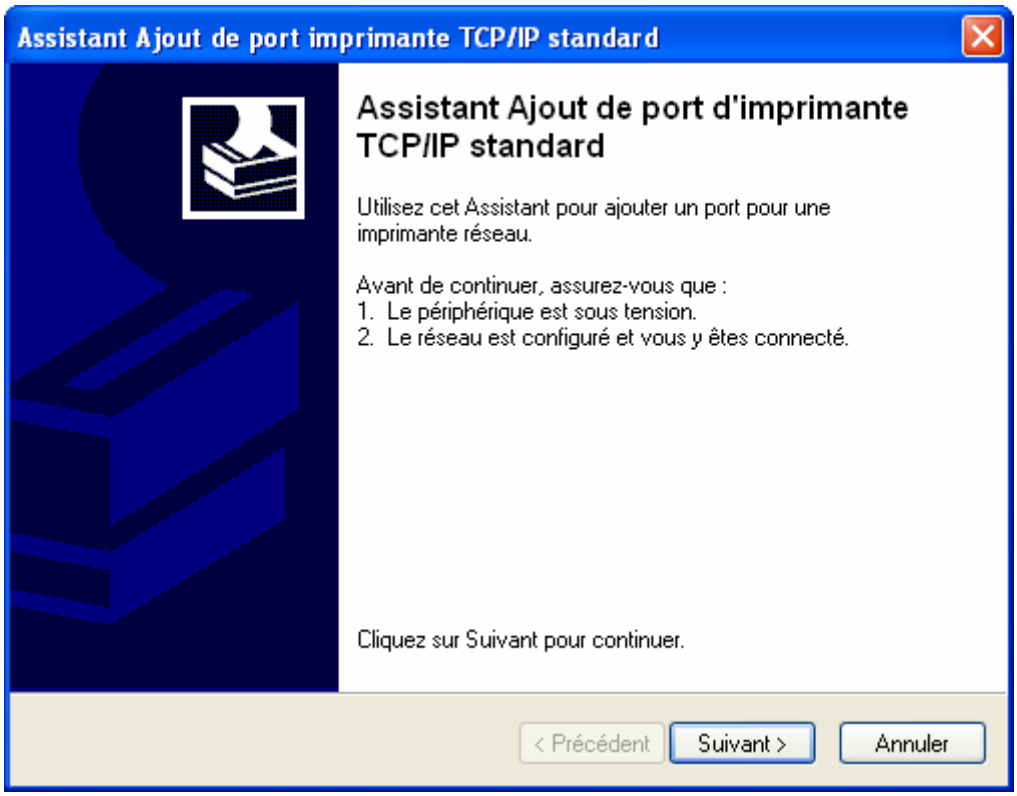
Remarque : ne cochez pas la case ***Détection et installation automatique de l'imprimante Plug-and-Play****.*


Assistant Ajout d'imprimante
Imprimante réseau ou locale
L'Assistant doit connaître le type d'imprimante à installer.
Sélectionnez l'option qui décrit l'imprimante que vous voulez utiliser :
Une imprimante locale connectée à cet ordinateur
Détection et installation automatique de l'imprimante Plug-and-Play
Une imprimante réseau ou une imprimante connectée à un autre ordinateur
Pour configurer une imprimante réseau qui n'est pas connectée à un serveur d'impression, utilisez l'option Imprimante locale.
< Précédent
Suivant >
Annuler

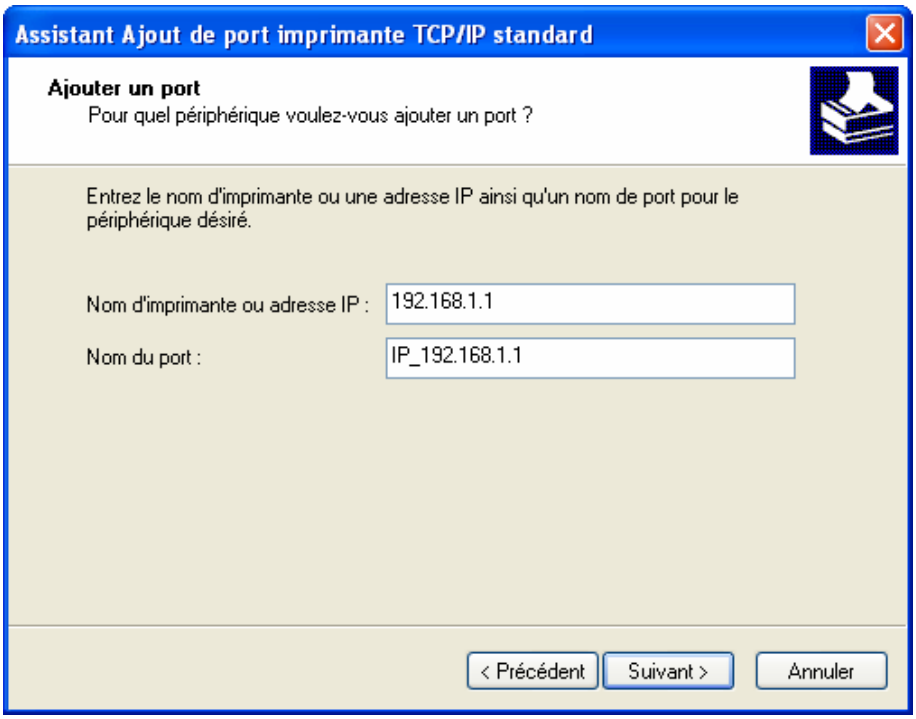
5. Sélectionnez **Créer un nouveau port**, puis dans la liste déroulante **Type de port**, sélectionnez **Standard TCP/IP Port**. Cliquez sur **Suivant**.


Assistant Ajout d'imprimante
Sélectionnez un port d'imprimante
Les ordinateurs communiquent avec les imprimantes via les ports.
Sélectionnez le port auquel vous souhaitez connecter votre imprimante. Si celui-ci n'est pas dans la liste, vous pouvez créer un nouveau port.
Utiliser le port suivant :
LPT1: (Port imprimante recommandé)
Remarque : la plupart des ordinateurs utilisent le port LPT1: pour communiquer avec une imprimante locale. Le connecteur de ce port ressemble à ceci :
Créer un nouveau port :
Type de port :
Standard TCP/IP Port
< Précédent
Suivant >
Annuler

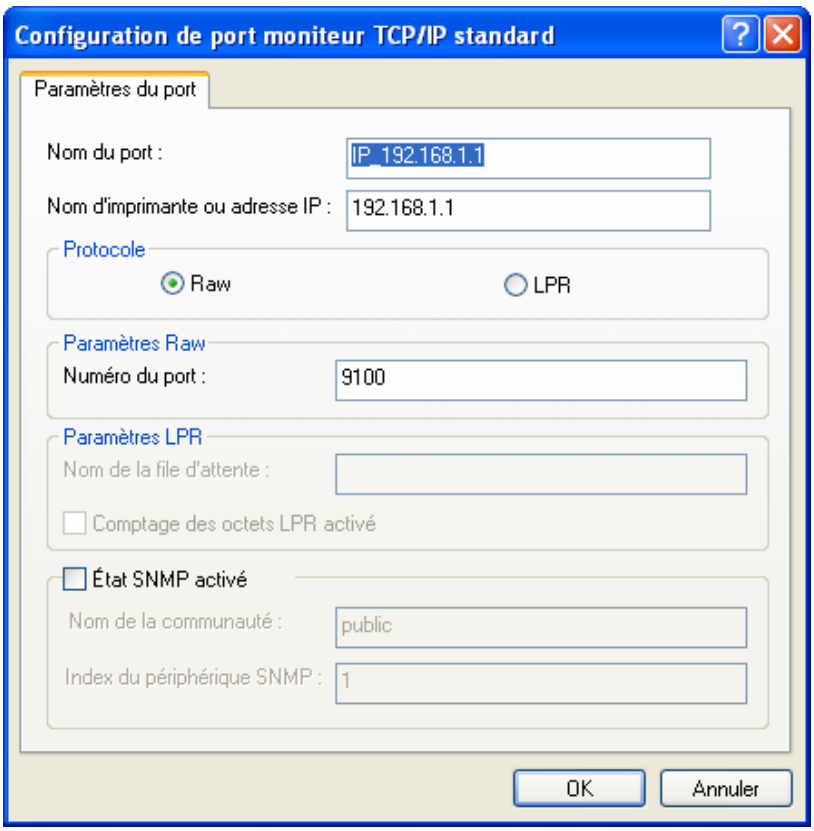
6. Vous allez désormais ajouter un port pour votre imprimante. Cliquez sur **Suivant**.


Assistant Ajout de port imprimante TCP/IP standard
Assistant Ajout de port d'imprimante TCP/IP standard
Utilisez cet Assistant pour ajouter un port pour une imprimante réseau.
Avant de continuer, assurez-vous que :
1. Le périphérique est sous tension.
2. Le réseau est configuré et vous y êtes connecté.
Cliquez sur Suivant pour continuer.
< Précédent
Suivant >
Annuler

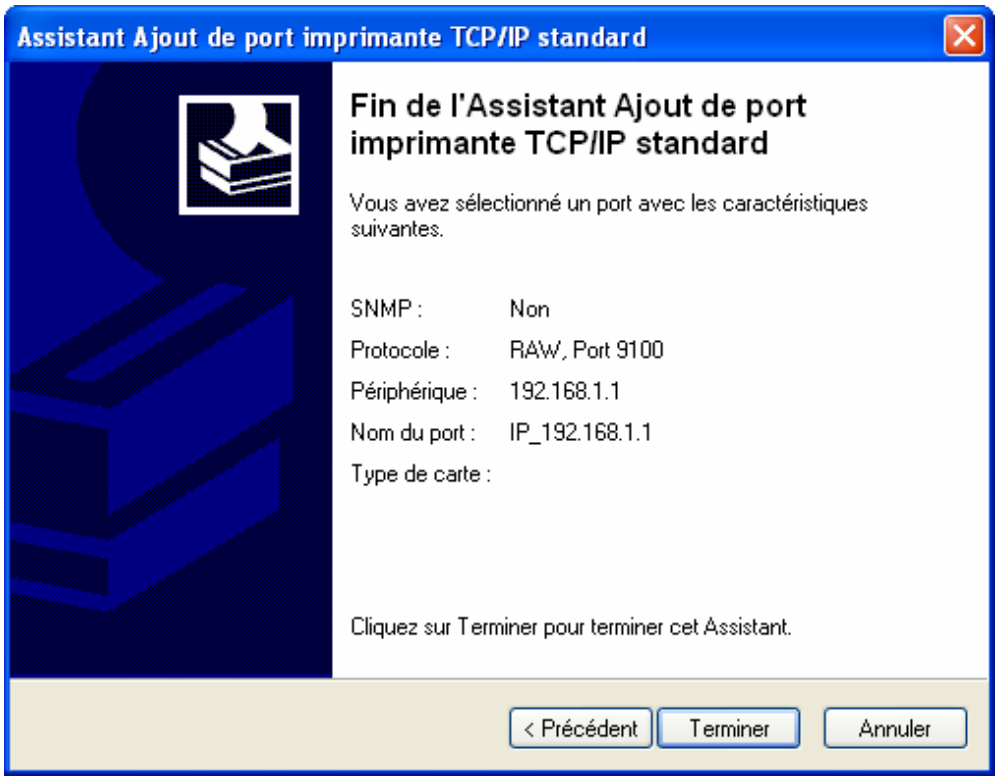
7. Dans le champ **Nom d'imprimante ou adresse IP** (192.168.1.1, dans notre exemple), saisissez l'adresse IP du routeur. Le nom du port est automatiquement créé. Cliquez sur **Suivant**.


Assistant Ajout de port imprimante TCP/IP standard
Ajouter un port
Pour quel périphérique voulez-vous ajouter un port ?
Entrez le nom d'imprimante ou une adresse IP ainsi qu'un nom de port pour le périphérique désiré.
Nom d'imprimante ou adresse IP :
192.168.1.1
Nom du port :
IP_192.168.1.1
< Précédent
Suivant >
Annuler

8. Dans la partie **Type de périphérique**, sélectionnez **Personnalisé**, puis cliquez sur le bouton **Paramètres…**.
9. Dans la partie **Protocole**, sélectionnez **Raw**.
10. Saisissez le numéro de port figurant dans **Maintenance** > **Périphériques USB** > **Imprimantes USB**. Cliquez sur **OK**, puis cliquez sur **Suivant**.

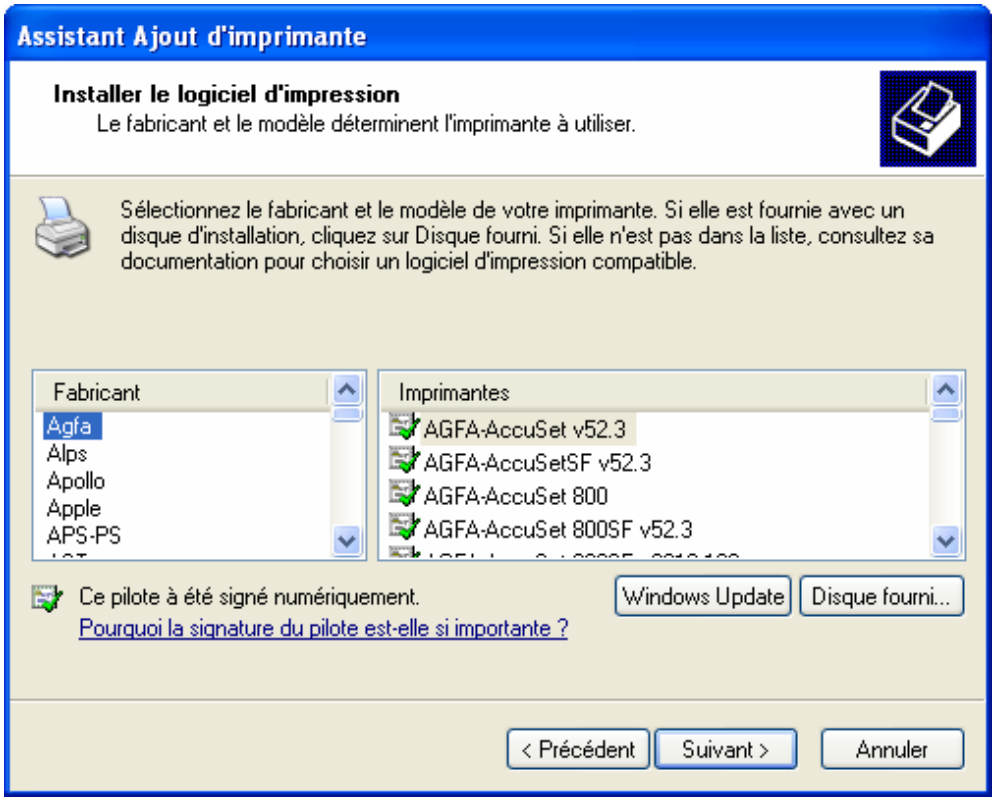


11. Votre port imprimante a bien été ajouté. Cliquez alors sur **Terminer**.

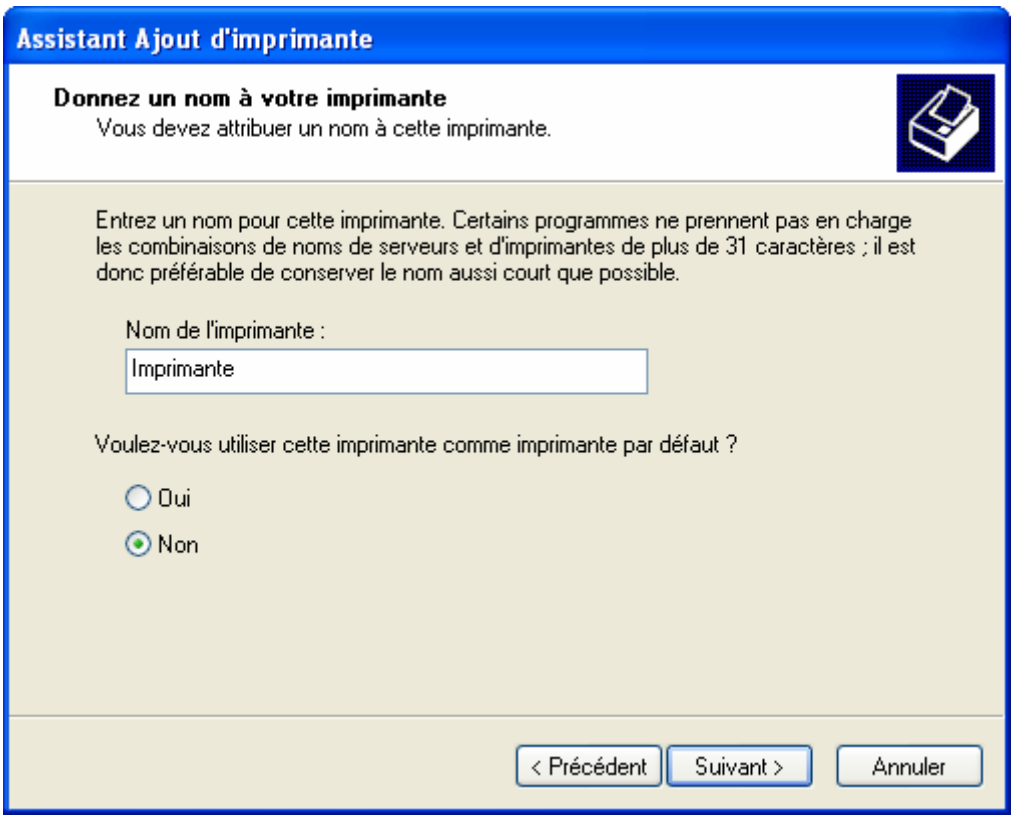

Assistant Ajout de port imprimante TCP/IP standard
Fin de l'Assistant Ajout de port imprimante TCP/IP standard
Vous avez sélectionné un port avec les caractéristiques suivantes.
SNMP : Non
Protocole : RAW, Port 9100
Périphérique : 192.168.1.1
Nom du port : IP_192.168.1.1
Type de carte :
Cliquez sur Terminer pour terminer cet Assistant.
< Précédent
Terminer
Annuler

12. Installez ensuite les pilotes de l'imprimante en sélectionnant tour à tour le fabricant, puis votre modèle d'imprimante. Cliquez sur **Suivant**.

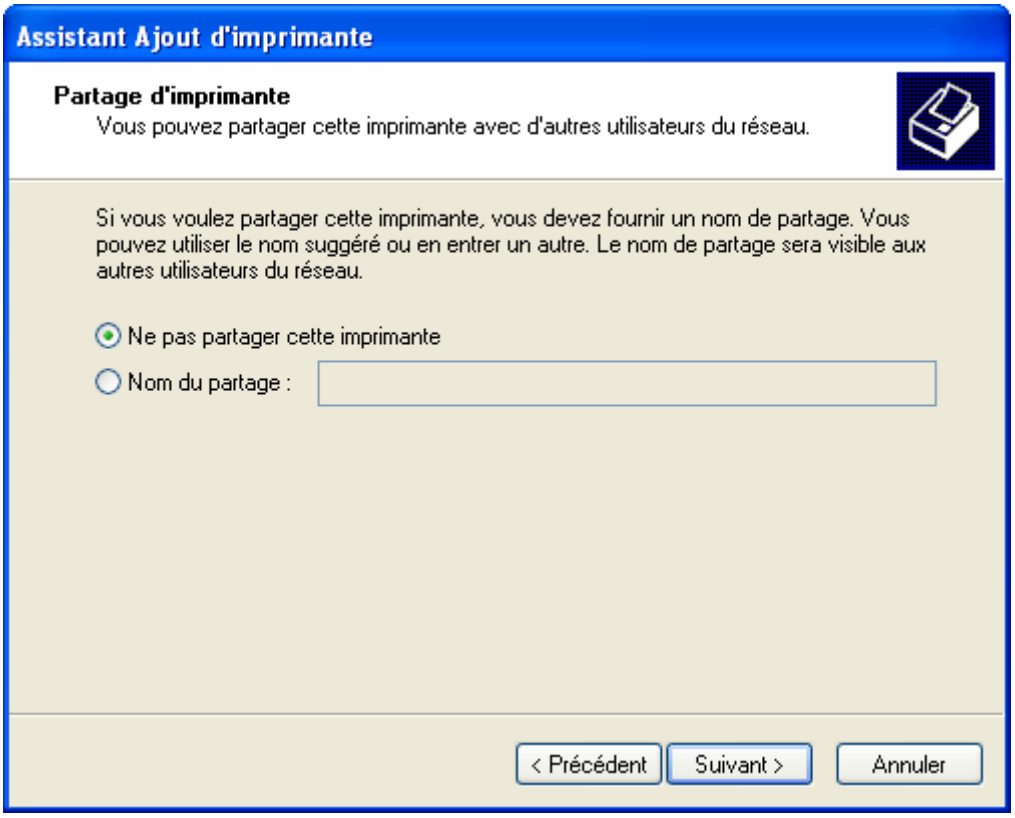
Remarque : si l'imprimante que vous souhaitez installer ne fait pas partie de cette liste, cliquez sur ***Disque fourni…****, puis installez les pilotes de votre imprimante grâce au CD-ROM du fabricant livré avec votre matériel.*


Assistant Ajout d'imprimante
Installer le logiciel d'impression
Le fabricant et le modèle déterminent l'imprimante à utiliser.
Sélectionnez le fabricant et le modèle de votre imprimante. Si elle est fournie avec un disque d'installation, cliquez sur Disque fourni. Si elle n'est pas dans la liste, consultez sa documentation pour choisir un logiciel d'impression compatible.
Fabricant
Agfa
Alps
Apollo
Apple
APS-PS
Imprimantes
AGFA-AccuSet v52.3
AGFA-AccuSetSF v52.3
AGFA-AccuSet 800
AGFA-AccuSet 800SF v52.3
Ce pilote à été signé numériquement.
Pourquoi la signature du pilote est-elle si importante ?
Windows Update
Disque fourni...
< Précédent
Suivant >
Annuler

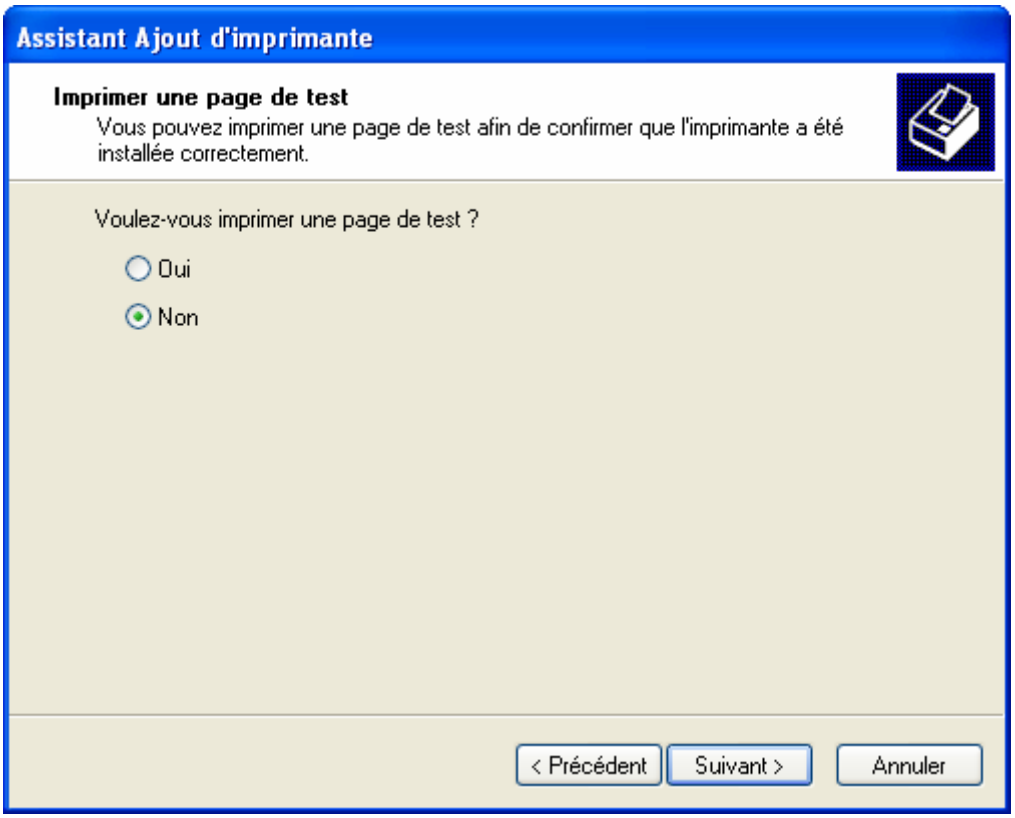
13. Sélectionnez **Conserver le pilote existant (recommandé)**, puis cliquez sur **Suivant**.
14. Si vous le souhaitez, modifiez le nom de votre imprimante, puis cliquez sur **Suivant**.


Assistant Ajout d'imprimante
Donnez un nom à votre imprimante
Vous devez attribuer un nom à cette imprimante.
Entrez un nom pour cette imprimante. Certains programmes ne prennent pas en charge les combinaisons de noms de serveurs et d'imprimantes de plus de 31 caractères ; il est donc préférable de conserver le nom aussi court que possible.
Nom de l'imprimante :
Imprimante
Voulez-vous utiliser cette imprimante comme imprimante par défaut ?
Oui
Non
< Précédent
Suivant >
Annuler

15. En fonction de vos besoins, indiquez si vous souhaitez ou non partager cette imprimante (dans notre exemple, nous choisissons de ne pas la partager). Cliquez sur **Suivant**.


Assistant Ajout d'imprimante
Partage d'imprimante
Vous pouvez partager cette imprimante avec d'autres utilisateurs du réseau.
Si vous voulez partager cette imprimante, vous devez fournir un nom de partage. Vous pouvez utiliser le nom suggéré ou en entrer un autre. Le nom de partage sera visible aux autres utilisateurs du réseau.
Ne pas partager cette imprimante
Nom du partage :
< Précédent
Suivant >
Annuler

16. Indiquez si vous souhaitez ou non imprimer une page de test. Cliquez sur **Suivant**.


Assistant Ajout d'imprimante
Imprimer une page de test
Vous pouvez imprimer une page de test afin de confirmer que l'imprimante a été installée correctement.
Voulez-vous imprimer une page de test ?
Oui
Non
< Précédent
Suivant >
Annuler

17. Une fenêtre récapitulative apparaît. Cliquez sur **Terminer** pour fermer l'Assistant.
18. Votre page de test, si vous avez choisi de l'imprimer, va être envoyée à l'imprimante. Si cela fonctionne, cliquez sur **OK**.
19. L'imprimante est bien connectée à votre ordinateur, disponible et prête à répondre à vos requêtes d'impression.

Annexes

Liste des webcams compatibles

Fabricant	Modèle
Aiptek	Pocket DV
Aiptek	PocketDV 3300
Amitech	AWK-300
Archos	Jukebox Multimedia 20
Askey	VC010 (Type 1)
Askey	VC010 (type 2)
Askey	VC080
AVerMedia Technologies, Inc.	Avercam Elite
Bruneau	Digi Tech
Canon Inc.	Digital IXUS V2
Canyon	WCAM 21
Casio	EX-P505
CASIO Computer CO LTD	KP-C50
Chicony Electronics CO., Ltd	TwinkleCam
Concord	Eye-Q Duo 1300
Connectix	QuickCam VC
Creative	Creative NoteBook PD1170
Creative	Creative NX Pro PD1130
Creative	Creative NX Pro PD1131
Creative	PC-CAM 880
Creative	Webcam Notebook PD1171
Creative	Webcam NX Pro PD1130
Creative	Webcam NX Ultra
Creative Labs	WebCam Plus (Model CT6840)
Creative Labs	WebCam Plus (Model PD0040)
Creative Labs	WebCam Pro eX
Creative Technology Ltd	Creative WebCam Go Mini
D-Link	DSB-C100

DEXTRA	InfoCam
DEXXA	webcam
DigitalDream	l'espion
Divio	nw802lq based webcam
DNT GmbH	DVB-T EuroMini 100
Etoms	Etoms-based camera + image sensor
Ezonics	EZ USB Cam II
flexi cam	flexicam
Fuji Photo Film Co., Ltd	FinePix S304 (3800)
FUJIFILM Camera	FUJIFILM EX-10/EX-20
Genius	VideoCam Express
Genius	VideoCAM Express V2
Genius	VideoCAM Web (version 1)
Genius KYE	VideoCAM GE111
Hewlett Packard	Photosmart M307
Hewlett Packard	Photosmart R607
Intel	Create & Share Camera Pack
Intel	CS330
Intel	Play Me2Cam
Intel Corp.	Intel Easy PC Camera CS110
JVC	GR-DVP7
JVC	GZ-MC200
Kensington	Kensington VideoCam PC Camera
Kensington	VideoCAM
Kensington	VideoCAM 67017
Konica Corporation	Digital Color Camera
Labtec	WebCam
Labtec	Webcam Labtec Pro
LifeView	CapView
Lifeview	Robocam
Logitech	Labtec
Logitech	QuickCam Messenger
Logitech	QuickCam Chat
Logitech	QuickCam Communicate
Logitech	QuickCam Express

Logitech	QuickCam Express (2003+ newer model)
Logitech	QuickCam for Notebooks Pro
Logitech	QuickCam Pro 3000
Logitech	QuickCam Pro 4000
Logitech	QuickCam Zoom
Maxell	Maxell PenCam Sdram LE
Maxxtro	PC Camera
Maxxtro	USB PC Camera
Meade	MicrOcular Biolux NG
Meade	MicrOcular1 Biolux NG
MEADE-Bresser	Biolux 654 MicrOcular
Mediaforte	MV300
Medion	MD40820 - Digital Camera
Medion Tevion	USB Webcam
Mercury	2.1 Deluxe Classic Cam
Mercury	3.1 Deluxe Classic Cam
Mercury	mercury pocket digital camera
MSI	MSI VOX USB 2.0 Analog TV
Mustek	VCAM-300
Nikon	Nikon DSC E885
Olympus	Camedia Digital Camera D-545
Orite	I-Cam MC311P
Panasonic	DVC-Storage
Philips	PCA645VC
Philips	PCA646VC
Philips	PCVC665K
Philips	PCVC675K
Philips	PCVC680K
Philips	PCVC690K
Philips	PCVC720K
Philips	PCVC740K
Philips	PCVC740K ToUcam Pro
Philips	PCVC830K (ToUcam FUN II)
Philips	PCVC840K
Philips	ToUcam II PCVC820K 00

Philips webcam / audio	PCVC 750K
Pinnacle	PCTV USB2
Pixart Imaging, Inc.	Sangha SN-510
Plustek	Opticam 300U
Polaroid	Polaroid ION 230 (PC camera mode)
Prochips	PCC-2200K/W
Q-TEC	Webcam 100 USB
Samsung Techwin	Samsung Digimax 370
Sangha	Q cam Sangha
Sangha	X cam sangha
Sitecom	VP-001 Easycam
SONiX	SN9C101,2,3 PC Camera Controllers
Sonix (et al)	PCCam 168
Sony	DCR-PC120BT
Sony	PC9E
Sony	Sony DSC
Sony DSC	DCR-TRV33E
STMicroelectronics	USB Dual-mode Camera
Swann	SmartCAM Deluxe
SWEEX	SWEEX WEBCAM
TerraTec	TerraCAM 2move
TerraTec	TerraCAM PRO
TerraTec	TerraCAM USB
Terratec	USB Camera
TerraTec GmbH	Cinergy T2
Toshiba	PDR-3330
Triplex Corporation	i-mini PC camera
Trust	Spacec@m 100
Trust	Spacec@m 200
Trust	Spacec@m Lite
Trust	Spacec@m 320
Trust	SpyC@m 300XS
usb digital still	camera
Veo	Stingray
Veo	Stingray USB camera

View-Cam	M6215
ViewQuest Technologies, Inc or BTC	DSC 5300Z CCD 5.2 mega pixels Digital Camera
ViewQuest Technologies, Inc.	1.3M DigitalCAM
Wasam	Wa350R
Z-Star Microelectronics Corp.	Integrated Laptop Webcam
Zoom Telephonics	ZoomCam USB 1595

Liste des imprimantes compatibles

Fabricant	Modèle
Brother	DCP-1000
Brother	HL-1250
Brother	HL-1450
Canon	BJ F300
Canon	BJC-3000
Canon	BJC-6100
Canon	BJC-85
Canon	i865
Canon	S100SP
Canon	S450
Compaq	IJ600
Compaq	IJ650
Digitus	USB to IEEE 1284 PRINTER CABLE
Epson	C64 photo edition
Epson	C62
Epson	EPL5900
Epson	Styles Photo RX600
Epson	Stylus C84
Epson	Stylus CX3650
Epson	Stylus C40UX
Epson	Stylus C44UX
Epson	Stylus C80
Epson	Stylus C82
Epson	Stylus Color 680
Epson	Stylus Color 740
Epson	Stylus Color 777
Epson	Stylus Color 860
Epson	Stylus Color 980
Epson	Stylus Photo 780
Epson	Stylus Photo 870
Epson	Stylus Photo 895EX

Epson	Stylus Photo 1200
Epson	Stylus Photo 1270
Epson	USB Printer
Epson	Epson C82
Hewlett Packard	hp 930c
Hewlett Packard	HP Designjet500 42 inch
Hewlett Packard	OfficeJet V40
Hewlett Packard	Deskjet 3650
Hewlett Packard	DeskJet 640C
Hewlett Packard	DeskJet 648C
Hewlett Packard	DeskJet 656C
Hewlett Packard	DeskJet 660C
Hewlett Packard	DeskJet 810C
Hewlett Packard	DeskJet 812C
Hewlett Packard	DeskJet 815C
Hewlett Packard	DeskJet 840C
Hewlett Packard	DeskJet 842C
Hewlett Packard	DeskJet 845C
Hewlett Packard	DeskJet 895C
Hewlett Packard	DeskJet 930C
Hewlett Packard	DeskJet 932C
Hewlett Packard	DeskJet 940C
Hewlett Packard	Deskjet 959C
Hewlett Packard	DeskJet 970Cse
Hewlett Packard	DeskJet 980Cxi (professional series)
Hewlett Packard	DeskJet 1220C
Hewlett Packard	DeskJet 3820
Hewlett Packard	DeskJet 5550
Hewlett Packard	DeskJet 5652
Hewlett Packard	DeskJet 6540
Hewlett Packard	HP color LaserJet 2550 series
Hewlett Packard	HP LaserJet 1010
Hewlett Packard	HP LaserJet 1300
Hewlett Packard	HP LaserJet 3300/3310/3320
Hewlett Packard	HP LaserJet 4050

Hewlett Packard	Photosmart 7350
Hewlett Packard	Photosmart 7760
Hewlett Packard	Photosmart P1100
Hewlett Packard	PSC1110
Hewlett Packard	PSC2110
Lexmark	inkjet (x-73)
Lexmark	Optra E3
LexMark	Z32 Color Jetprinter
LexMark	Z52
LexMark	Z53
Olivetti	NomadJet 100
Samsung	ML-1410
Samsung	ML-1740
Samsung	Laser Printer ML-4600
Samsung	Laser Printer ML-1200 Series
Samsung	ML-1710 Series
Xerox	Docuprint P8ex

DECLARATION DE CONFORMITE

Nom du constructeur : BeWAN systems

Adresse : 16, rue du Moulin des Bruyères **Téléphone :** +33 1 43 34 69 20

Code postal : 92400 **Télécopie :** +33 1 46 91 03 71

Localité : Courbevoie - France

Identification du produit

Nom : BeWAN Secure 50 / BeWAN Secure M50

Type : Routeur 10/100 BaseTx

Référence : BWSEC-50 / BWSEC-M50

BeWAN systems déclare sous son entière responsabilité que le produit décrit ci-dessus est en conformité avec les exigences essentielles de la Directive **R&TTE 1999/5/CE** sur les équipements hertziens et les équipements terminaux de télécommunications.

Le produit est également conforme aux exigences définies par la Directive **89/336/CE** (amendée par les Directives **91/263/CE**, **92/31/CE** et **93/68/CE**) concernant la compatibilité électromagnétique et par la Directive **73/23/CE** (amendée par la Directive **93/68/CE**) sur les basses tensions, la protection de la santé et de la sécurité de l'utilisateur.

Le produit est conforme aux normes européennes harmonisées suivantes :

EN 55022:1998 + A1:2000 + A2:2003, Class B
EN 60950-1:2001
EN 61000-3-2 edition 2:2000
EN 61000-3-3:1995 + A1:2001
IEC 61000-4-2:1995 + A1:1998 + A2:2001
IEC 61000-4-3:2002 + A1:2002
IEC 61000-4-4:1995 + A1:2001
IEC 61000-4-5:1995 + A1:2001
IEC 61000-4-6:1996 + A1:2001
IEC 61000-4-11:1994 +A1:2001

Le marquage CE est apposé sur le produit.

Information supplémentaire : le produit a été testé dans une configuration standard.

Conformité RoHS (Restrictions of Hazardous Substances)

BeWAN systems déclare que le produit est conforme à la Directive RoHS **2002/95/CE** de l'Union européenne relative à la limitation de l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques : plomb (Pb), cadmium (Cd), mercure (Hg), chrome hexavalent (Cr VI), polybromobiphényles (PBB), polybromodiphényléthers (PBDE).

Date : Juillet 2006

Eric TEISSANDIER
Président du Conseil d'Administration

DECLARATION DE CONFORMITE

Nom du constructeur : BeWAN systems

Adresse : 16, rue du Moulin des Bruyères **Téléphone :** +33 1 43 34 69 20

Code postal : 92400 **Télécopie :** +33 1 46 91 03 71

Localité : Courbevoie - France

Identification du produit

Nom : BeWAN Secure 50G / BeWAN Secure M50G

Type : Routeur 10/100 BaseTx + Wi-Fi (IEEE 802.11g)

Référence : BWSEC-50G / BWSEC-M50G

BeWAN systems déclare sous son entière responsabilité que le produit décrit ci-dessus est en conformité avec les exigences essentielles de la Directive **R&TTE 1999/5/CE** sur les équipements hertziens et les équipements terminaux de télécommunications.

Le produit est également conforme aux exigences définies par la Directive **89/336/CE** (amendée par les Directives **91/263/CE**, **92/31/CE** et **93/68/CE**) concernant la compatibilité électromagnétique et par la Directive **73/23/CE** (amendée par la Directive **93/68/CE**) sur les basses tensions, la protection de la santé et de la sécurité de l'utilisateur. Le produit garantit l'utilisation efficace du spectre attribué aux équipements radioélectriques pour éviter les interférences dommageables.

Le produit est conforme aux normes européennes harmonisées suivantes :

EN 300 328 v1.6.1:2004
EN 301 489-01 v1.5.1:2004
EN 301 489-17 v1.2.1:2002
EN 55022:1998 + A1:2000 + A2:2003, Class B
EN 60950-1:2001
EN 61000-3-2 edition 2:2000
EN 61000-3-3:1995 + A1:2001
IEC 61000-4-2:1995 + A1:1998 + A2:2001
IEC 61000-4-3:2002 + A1:2002
IEC 61000-4-4:1995 + A1:2001
IEC 61000-4-5:1995 + A1:2001
IEC 61000-4-6:1996 + A1:2001
IEC 61000-4-11:1994 +A1:2001

Le marquage CE est apposé sur le produit.

Information supplémentaire : le produit a été testé dans une configuration standard.

Conformité RoHS (Restrictions of Hazardous Substances)

BeWAN systems déclare que le produit est conforme à la Directive RoHS **2002/95/CE** de l'Union européenne relative à la limitation de l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques : plomb (Pb), cadmium (Cd), mercure (Hg), chrome hexavalent (Cr VI), polybromobiphényles (PBB), polybromodiphényléthers (PBDE).

Date : Juillet 2006

Eric TEISSANDIER
Président du Conseil d'Administration